Adrian Munteanu, Valerică Greavu Şerban

Reţele locale de calculatoare

Proiectare şi administrare

POLIROM
2003

Adrian Munteanu (n. 1970) a absolvit Facultatea de Ştiinţe Economice Iaşi, secţia Contabilitate şi Informatică de Gestiune. În prezent este lector doctor şi predă disciplinele „Reţele de calculatoare" şi „Auditul sistemelor informaţionale" în cadrul Catedrei de Informatică Economică, Facultatea de Economie şi Administrarea Afacerilor (www.feaa.uaic.ro), Universitatea „Al.I. Cuza" Iaşi.

Valerică Greavu Şerban (n. 1976) a absolvit Facultatea de Ştiinţe Economice Iaşi, secţia Contabilitate şi Informatică de Gestiune. În prezent este administrator de reţea la Facultatea de Economie şi Administrarea Afacerilor şi doctorand în domeniul informaticii economice.

© 2003 by Editura POLIROM

www.polirom.ro

Editura POLIROM
Iaşi, B-dul Carol I nr. 4, P.O. BOX 266, 700506
Bucureşti, B-dul I.C. Brătianu nr. 6, et. 7, ap. 33, O.P. 37 ; P.O. BOX 1-728, 030174

Descrierea CIP a Bibliotecii Naţionale a României :

MUNTEANU, ADRIAN

Reţele locale de calculatoare : proiectare şi administrare / Adrian Munteanu, Valerică Greavu Şerban – Iaşi : Polirom, 2003

304 p. ; 24 cm

ISBN : 973-681-457-2

I. Greavu Şerban, Valerică

004.732(100)

Printed in ROMANIA

Preambul

De ce ne-am apucat de scris o astfel de carte cînd oricum există ofertă? Toată lumea este de acord că între teorie şi practică sînt diferenţe. Problema este că, teoretic, golul dintre teorie şi practică este ceva mai mic decît cel care există în practică.

De-a lungul ultimilor ani am îmbinat munca fizică cu cea ştiinţifică în catedră şi facultate pe această temă. Pornind de aici, am zis că nu ar fi rău să punem pe hîrtie ceea ce am acumulat. Cele 300 de pagini cuprind lucruri cunoscute. Sînt culese din cărţi şi din experienţa noastră practică. Pentru că nu este de ici de colo să lucrezi într-o instituţie care are o reţea cu o duzină de servere, peste 400 de staţii şi aproximativ 10.000 de utilizatori. Şi, spre mulţumirea noastră, reţeaua asta chiar funcţionează! Cartea se doreşte un ghid, un how to pentru cei care doresc să se iniţieze în acest domeniu.

Am început cu puţină teorie pentru că este nevoie de un astfel de fundament, dar am cuprins în mai puţin de 100 de pagini ceea ce am considerat că trebuie cunoscut despre anumite tehnologii. Nu am abordat subiectele care se întîlnesc în alte cărţi despre reţele, dar mai rar în practică (tehnologia Token Ring de exemplu).

Ne-am axat mai mult pe partea practică: *care sînt echipamentele folosite într-o reţea, ce reprezintă adresele IP şi cum se calculează, modul de funcţionare al switch-urilor şi reţele virtuale cu o scurtă iniţiere în sistemul de operare al switch-urilor CISCO, protocoale pentru rutare şi configurarea routerelor, proiectarea unei reţele şi instrumente pentru proiectare şi, nu în ultimul rînd, ce pot face script-urile pentru Windows-ul 2000 Server şi XP*. Nu avem pretenţia că am epuizat tot ce ţine de acest subiect, pentru că nu ne-am propus aşa ceva. După cum veţi observa, pe lîngă exemplele oferite, cartea este presărată cu o mulţime de trimiteri la adrese de pe Web.

Nu ne adresăm numai *avansaţilor*, ci şi celor care vor să se apuce de treabă, dar nu ştiu de unde să înceapă şi cum să continue.

Autorii

Iaşi, iulie 2003

Tablă de materii

Preambul 9

Partea I
Arhitecturi şi standarde

Capitolul 1
Modele şi standarde 13
1.1. A fost odată 13
1.2. Definirea reţelelor 16
1.2.1. Local Area Network (LAN - reţele locale) 17
1.2.2. Wide Area Network (WAN - reţele cu arie mare de întindere) 20
1.3. Modelul de referinţă OSI 20
1.4. Modelul TCP/IP 24

Capitolul 2
Infrastructura reţelei 27
2.1. Cartela de reţea 27
2.2. Medii de transmisie 28
2.3. Echipamente de transmisie a datelor 30

Capitolul 3
Nivelul legătură date 33
3.1. Funcţiile MAC 34
3.2. Încadrarea (*framing*) şi standardul Ethernet 35
3.2.1. Cadrul Ethernet 36
3.2.2. Half-Duplex Ethernet (CSMA/CD Access Protocol) 37
3.2.3. Full-Duplex Ethernet 40
3.3. FDDI 41
3.4. Domenii de coliziune 43

Capitolul 4
Nivelul reţea 47
4.1. Identificarea traseului 47
4.2. Protocolul IP 48

4.3. Adresarea IP 51
4.4. Adresarea IP în subrețele 54
4.5. Agregarea adreselor IP și NAT 57

Capitolul 5

Nivelul transport 59
5.1. TCP Transmission Control Protocol 60
5.2. UDP - User Datagram Protocol 64
5.3. ARP - protocolul de rezoluție a adresei 65
5.4. ICMP - protocolul mesajelor de control 68

Capitolul 6

Nivelurile sesiune și prezentare 71
6.1. Câteva considerații generale despre o sesiune 71
6.2. Prezentare 72

Capitolul 7

Nivelul aplicație 75
7.1. DNS - Domain Name System 75
7.2. SNMP - Protocolul simplu pentru administrarea rețelelor 77
7.3. Poșta electronică 78
7.4. File Transfer Protocol (Protocol pentru transferul fișierelor) 80
7.5. World Wide Web 81

Partea a II-a
Proiectarea rețelelor de calculatoare

Capitolul 8

Cablarea structurată a unei rețele de calculatoare 85
8.1. Standardul ANSI/TIA/EIA 568 85
8.2. Instalarea cablurilor 88
8.3. Factori care afectează semnalele dintr-o rețea 91
8.4. 10BaseT (Ethernet) 96
8.5. 100 BaseTX (Fast Ethernet) 97

Capitolul 9

Comutarea pachetelor în rețelele de calculatoare 101
9.1. Funcțiile unui switch 101
9.2. Funcționarea switch-ului 103
9.3. Metode de comutare a pachetelor 105
9.4. Spanning Tree Protocol (STP) 106

Capitolul 10

Rețele virtuale 109
10.1. Tipologia VLAN-urilor 109
10.2. Configurarea VLAN-urilor 113
10.3. VLAN Trunking Protocol (VTP) 113
10.4. Comenzile IOS 115
10.5. Exemplu 120

Capitolul 11

Privire generală asupra routerelor ... 125
11.1. Componentele routerului şi moduri de configurare ... 125
11.2. Pornirea unui router ... 127
11.3. Configurarea routerului ... 129
11.4. Accesul la alte routere ... 129
11.5. Protocoale pentru rutare ... 130
11.6. RIP - Routing Information Protocol ... 134
11.7. IGRP - Interior Gateway Routing Protocol ... 134
11.8. OSPF - Open Shortest Path First ... 135
11.9. Comenzi IOS ... 135
11.10. Studiu de caz ... 144

Capitolul 12

Proiectarea şi administrarea reţelelor ... 153
12.1. Proiectarea structurată a unei reţele de calculatoare ... 153
12.2. Securitatea reţelei ... 161
12.2.1. Aspecte legislative ... 161
12.2.2. Tipuri de atacuri într-o reţea ... 166
12.2.3. Mecanisme de protecţie ... 175
12.3. Proiectarea unei reţele. Studiu de caz ... 180

Capitolul 13 ... 187

Instalarea şi configurarea logică a unei reţele locale ... 187
13.1. Care este cel mai bun sistem de operare? ! ... 188
13.2. Instalarea Windows 2000 Server ... 192
13.3. Configurarea serverului W2 în vederea realizării unui domeniu W2 ... 201
13.4. Crearea unui server pentru un nou domeniu ... 209
13.5. Instalarea Windows XP în mod automat ... 213
13.6. Configurarea Active Directory. Crearea utilizatorilor. Definirea politicilor de securitate ... 232
13.7. Instalarea şi configurarea unui server de Web ... 258
13.8. Configurarea serverului ca un Gateway ... 260
13.9. Monitorizarea şi înregistrarea activităţii ... 262
13.10. Instrumente pentru depanare ... 268

Capitolul 14

Utilitare de administrare ... 273
14.1. Utilitare pentru accesul centralizat la resursele reţelei ... 273
14.2. Utilitare de monitorizare a traficului ... 274
14.3. Utilitare pentru accesul la WMI ... 275
14.4. Utilitare pentru conectarea la distanţă ... 276
14.5. Simulatoare şi instrumente de învăţare ... 278
14.6. Instrumente de proiectare a reţelelor ... 280

Anexă ... 285

Bibliografie ... 303

Partea I
Arhitecturi şi standarde

CAPITOLUL 1

Modele şi standarde

1.1. A fost odată

Cîte calculatoare sînt racordate la Internet? Se aproximează că ar fi peste 40 de milioane, dar nimeni nu are curajul să avanseze o cifră exactă. Popularitatea Internetului se datorează în principal World Wide Web-ului şi poştei electronice.

Pe *net* găseşti de toate. Este unul dintre motivele pentru care cei din branşă au ajuns să fie numiţi *netocraţi* după o evoluţie care a durat vreo 40 de ani. Cîţi dintre noi mai pot trăi astăzi fără porţia zilnică de Internet?

Toate lucrurile rele au şi o parte bună. De ce avem curajul să afirmăm aşa ceva? Pentru că, dacă în 1957 URSS nu ar fi plasat pe orbita Pamîntului primul satelit artificial (Sputnik), astăzi nu am fi avut probabil Internet. Ca răspuns la această palmă primită, în cadrul Departamentului de Apărare al SUA (DoD) ia fiinţă *Advanced Research Projects Agency* (*ARPA*). Americanii doreau să recupereze handicapul şi să devină lideri mondiali în domeniul ştiinţelor şi tehnologiilor cu aplicaţii militare. Cinci ani mai tîrziu (1962), *Paul Baran* de la Rand Corporation a fost însărcinat de către US Air Force să întocmească un studiu cu privire la posibilitatea menţinerii comenzilor şi controlului asupra rachetelor intercontinentale în cazul unui atac nuclear din partea URSS. Trebuia dezvoltată o reţea informatică descentralizată, astfel încît orice oraş american ar fi fost atacat, armata să poată declanşa un contraatac nuclear.

Baran descrie mai multe variante prin care se putea ajunge la rezultatul scontat, iar în final face o propunere concretă: comutarea pachetelor presupune descompunerea datelor în pachete (sau datagrame) care vor conţine informaţii cu privire la originea şi destinaţia lor. Aceste pachete vor circula prin reţea pînă cînd ajung la destinaţie.

Sfîrşitul anului 1968 şi începutul lui 1969 marchează naşterea Internetului. În 1968, National Physical Laboratory din Marea Britanie realizează şi testează prima reţea construită după principiile lui Baran. La scurt timp, Advanced Research Projects Agency din cadrul Pentagonului decide realizarea unei reţele mai mari. În toamna anului 1969, la UCLA se realizează primul nod al acestei reţele, iar pînă în decembrie mai apar încă 3: University of California (Los Angeles), SRI (Stanford), University of California (Santa Barbara) şi University of Utah. Această reţea va fi denumită ARPANET după numele sponsorului agenţiei Pentagonului. Cele patru noduri puteau transmite informaţii între ele prin intermediul unor linii dedicate şi chiar puteau fi programate de la distanţă.

Pînă în 1972 ARPANET va ajunge la 35 de noduri, principalul trafic al reţelei constînd în ştiri şi mesaje personale.

În acelaşi an, *Ray Tomlison* de la BBN realizează primul program de poştă electronică. Interesant este că acesta a fost folosit în principal pentru discuţii între împătimiţii de science fiction (lista se numea SF-Lovers).

Standardul original pe care se bazau comunicaţiile reţelei ARPA s-a numit NCP - Network Control Protocol. Însă pe măsură ce anii au trecut şi tehnica a avansat, *Vinton Cerf* de la Stanford împreună cu *Bob Kahn* de la DARPA (noua denumire a reţelei ARPA) au înlocuit, în 1973, NCP cu TCP/IP - Transmission Control Protocol/Internet Protocol. Acest nou protocol oferea suport pentru comunicaţie calculatoarelor cu arhitecturi diferite. Mai mult, TCP/IP a fost folosit pentru a lega între ele calculatoare care nu făceau parte din ARPANET (în 1983, reţeaua militară s-a desprins sub denumirea MILNet).

Anul 1976 este unul al realizărilor deosebite. Dr. *Robert M. Metcalfe* dezvoltă tehnologia Ethernet care permite transferul de date pe cablu coaxial. A fost o realizare crucială pentru domeniul reţelelor. În acelaşi an ia naştere SATNET reţeaua care lega SUA de Europa. Chiar dacă pare surprinzător, această reţea folosea sateliţii INTELSAT aflaţi în proprietatea unui consorţiu de ţări europene.

Trei ani mai tîrziu, un tînăr absolvent al Universităţii North Carolina, *Steve Bellovin*, împreună cu programatorii *Tom Truscott* şi *Jim Ellis* dezvoltă USENET. Era prima reţea descentralizată dedicată în exclusivitate ştirilor. Această reţea se baza pe protocolul UUCP (Unix-to-Unix CoPy) dezvoltat de AT&T Bell Labs şi distribuit împreună cu sistemul de operare Unix.

Similar cu USENET, reţeaua BITNET (*Because It's Time Network*) conecta mainframe-urile IBM din mediul educaţional pentru a oferi servicii de poştă electronică.

Despre anul 1983 putem spune că este anul Internet: se înfiinţează IAB - Internet Activities Board. Începînd cu prima zi a acestui an, toate calculatoarele conectate la ARPANET folosesc TCP/IP şi renunţă la NCP. În sprijinul IAB a venit Universitatea din Wisconsin care a creat Domain Name System - DNS. Acesta permitea pachetelor să fie direcţionate către un nume de domeniu unde i se aloca adresa IP corespunzătoare. Utilizatorii au putut astfel să acceseze mult mai uşor serverele reţelei.

Cercetările şi dezvoltările continuă pe parcursul următorilor ani. Astfel, autoritatea care dirijează evoluţia Internetului este **ISOC (Internet SOCiety)**[1], înfiinţată în ianuarie 1992, cu scopul de a promova utilizarea Internetului şi de a prelua administrarea sa. În cadrul acestei organizaţii, o parte din membri sînt reuniţi în cadrul **IAB (Internet Architecture Board)**[2] care are responsabilitatea tehnică a evoluţiei reţelei şi defineşte standardele Web. Membrii acestui consiliu au întîlniri regulate în care sînt acceptate noi standarde, alocă adresele şi păstrează o listă a numelor care trebuie să rămînă unice. Comunicările sînt puse la dispoziţie printr-o serie de rapoarte tehnice, numite **RFC**-uri (Request For Comments)[3], care sînt memorate online şi pot fi citite de oricine este interesat de ele.

Consiliul IAB este format din patru grupuri principale şi anume: **IRTF (Internet Research Task Force)** care are rolul de a rezolva problemele pe termen lung, **IETF**

1. www.isoc.org.
2. www.iab.org.
3. http://www.rfc-editor.org sau http://www.ietf.org/rfc.html.

(Internet Engineering Task Force) care are sarcina de a rezolva problemele pe termen scurt, **IESG (Internet Engineering Steering Group)** şi **IRSG (Internet Research Steering Group)**. Aceste grupuri sînt responsabile cu evaluarea şi testarea proiectelor şi standardelor propuse, pentru a determina dacă o propunere merită să devină un standard Internet.

Pe tot parcursul anilor care s-au scurs de atunci dezvoltările au continuat. Comunicarea în Internet a devenit o sursă inepuizabilă şi rapidă de documentare, depăşind complet toate celelalte surse de documentare. Internetul pune la dispoziţia utilizatorilor (cel puţin) cinci servicii extrem de importante şi anume:

1. poşta electronică (e-mail): poate fi folosită pentru a expedia mesaje unor persoane din orice colţ al lumii;
2. transferul fişierelor (ftp: *File Transfer Protocol*): este folosit la transferul fişierelor (text sau binare) între două calculatoare;
3. conectare la o maşină la distanţă (telnet, ssh, Terminal Services): folosit la deschiderea unor sesiuni de lucru pe maşini aflate la distanţă;
4. buletine de ştiri (usenet): utilizatorii se pot înscrie la grupuri de discuţii;
5. Word Wide Web (sau WWW): facilitează transferul informaţiei între servere Web.

Primele programe (browsere, clienţi de e-mail şi ftp) Internet aveau o interfaţă exclusiv bazată pe linia de comandă. Acest lucru a fost schimbat de World Wide Web, care oferă o prezentare grafică a Internetului fără a mai impune cunoaşterea unor comenzi cu sintaxa mai mult sau mai puţin complicată. Deşi utilizează Internetul pentru funcţionare, Web-ul se bazează pe un concept total diferit: hypertextul. Diferenţa între un text static (un articol de ziar) şi hypertext este uriaşă: în cazul hypertextului, calculatorul poate aduce direct pe ecran toate fragmentele la care textul curent are legături (cu doar un click!), fără a strica impresia de document unitar. Word Wide Web oferă hypertext şi, mai mult, depăşeşte simpla interconectare a documentelor text. Caracteristicile Web (JavaScript, CGI etc.) permit paginilor individuale de Web să interacţioneze cu utilizatorul, iar serverele Web pot crea pagini Web bazate pe informaţii dinamice.

WWW este, astăzi, cel mai „vizibil" instrument Internet. Web-ul prezintă informaţia sub forma de text şi grafică şi oferă afacerilor cea mai motivată raţiune pentru conectarea la Internet: uşurinţa şi rapiditatea comunicaţiilor.

Am început cu evoluţia reţelelor prin prisma Internetului dintr-un singur motiv: în cele mai multe cazuri, cei din afara branşei asociază reţelele cu Internetul. Şi nu cred că greşesc.

Pînă la apariţia Internetului, evoluţia reţelelor a fost la fel de interesantă.

În faza lor incipientă, reţelele nu se bazau pe o legătură fizică între calculatoare (*Sport-Shoe Networking*). Mediul de comunicaţie era discheta, iar viteza de transmisie era determinată de viteza de deplasare a utilizatorului de la un calculator la altul (de unde şi numele). Astăzi, am ajuns să discutăm de reţele pe fibră optică sau de cele fără fire. Întrebarea firească este *cum s-a ajuns aici*?

Firmele care deţineau calculatoare au fost nevoite să găsească o soluţie prin care să-şi poată partaja resursele, să obţină o fiabilitate ridicată prin accesul la echipamente şi să economisească bani. Toate aceste probleme au fost rezolvate prin dezvoltarea tehnologiilor reţelelor.

Dacă în anii '70-'80 cele mai multe companii puneau la dispoziţia angajaţilor terminale conectate la calculatoare puternice, popularitatea reţelelor a crescut în momentul în care reţelele formate din calculatoare personale au oferit un raport preţ/performanţă optim. Începînd cu anii '90 accesul de la distanţă la informaţii, comunicaţiile interpersonale şi divertismentul interactiv au contribuit decisiv la expansiunea reţelelor. La acestea se adaugă sistemele de operare disponibile comercial.

1.2. Definirea reţelelor

În termeni foarte simpli, o *reţea* reprezintă un sistem de oameni şi obiecte conectate între ele. Oriunde privim în jurul nostru putem observa un anumit tip de reţea (sistemul nervos, sistemul cardiovascular, sistemul de încălzire [sic]). Reţelele de comunicaţii sînt proiectate astfel încît două calculatoare, localizate oriunde în lume, să fie capabile să comunice între ele, indiferent de tipul acestora (PC, Mac, *mainframe* etc.). Acest lucru este posibil prin intermediul unei limbi comune, numită *protocol.*

Protocolul este definit ca un *set formal de reguli şi convenţii cu ajutorul cărora este guvernat schimbul de informaţii între echipamentele unei reţele.*

Majoritatea reţelelor sînt clasificate în LAN[1] (localizate de obicei într-o clădire, campus) sau WAN (acoperă o arie geografică mai mare). Ele sînt rezultatul dezvoltării aplicaţiilor pentru mediul afacerilor. Dar fiecare dintre aceste aplicaţii avea o manieră proprie de operare, independentă de calculator. Eficienţa dispărea în acest caz. Organizaţiile aveau nevoie de o soluţie care să rezolve următoarele probleme:

- cum să fie evitată duplicarea echipamentelor?
- cum se poate comunica eficient?
- cum se poate gestiona o reţea?

O primă soluţie la problemele organizaţiei a fost realizarea reţelelor locale (LAN). Deoarece puteau conecta toate staţiile de lucru şi perifericele dintr-o clădire, LAN-urile au făcut posibilă utilizarea eficientă a tehnologiilor informaţionale.

Însă, pe măsură ce calculatoarele au început să fie folosite pe scară tot mai largă în domeniul economic, LAN-urile nu mai erau suficiente. A apărut necesitatea schimbului de informaţii între organizaţii, iar soluţia a reprezentat-o apariţia WAN.

La început, dezvoltarea reţelelor LAN şi WAN a fost haotică. Anii '80 pot fi caracterizaţi printr-o expansiune extraordinară a reţelelor. Companiile au început să fie conştiente de economiile rezultate în urma folosirii tehnologiei reţelelor.

La mijlocul anilor '80 însă, această creştere s-a oprit brusc. Multe dintre tehnologiile folosite în reţele se bazau pe soluţii hard şi soft diferite, fapt care a dus la incompatibilitatea dintre acestea. Devenea din ce în ce mai dificilă comunicarea între reţelele care foloseau specificaţii diferite.

1. A apărut şi o denumire mai nouă: CAN - Campus Area Network.

1.2.1. Local Area Network (LAN - reţele locale)

Reţele de tip LAN (Local Area Network) reprezintă cea mai comună implementare a tehnologiei reţelelor pentru firmele de mărime mică-medie. O astfel de reţea se caracterizează prin :

- operare într-o arie geografică limitată ;
- permite accesul utilizatorilor la medii de transmisie cu lăţime de bandă mare ;
- oferă conectivitate continuă pentru serviciile locale ;
- conectează fizic echipamente adiacente.

Dacă privim acest tip de reţele prin prisma sistemelor de operare ce pot fi folosite, vom putea clasifica aceste reţele în *peer-to-peer* şi *reţele bazate pe servere*.

Reţelele peer-to-peer nu implică existenţa unui server care să asigure serviciile în reţea. Fiecare dintre calculatoarele reţelei poate îndeplini şi funcţia de server. Utilizatorul este cel care hotărăşte ce periferic sau informaţie doreşte să fie accesată şi de ceilalţi membri ai reţelei. Acest tip de reţele se pretează cel mai bine pentru firmele mici, unde, datorită complexităţii relativ reduse a activităţilor, nu este nevoie de servicii sofisticate.

La polul opus, reţelele bazate pe server(e) implică existenţa cel puţin a unui calculator care să joace rolul de server. În acest caz, informaţiile care trebuie partajate în cadrul firmei vor fi gestionate de server. Aceasta este soluţia adoptată de majoritatea firmelor şi ca urmare a posibilităţii gestionării centralizate a securităţii reţelei. Serverele dintr-o astfel de reţea pot îndeplini următoarele roluri :

- *servere de fişiere şi imprimare* - oferă un suport sigur pentru toate datele companiei şi gestionează tipărirea la imprimantele partajate în reţea ;
- *servere pentru aplicaţii* - asigură componenta cu acelaşi nume pentru aplicaţiile client-server. Exemple de astfel de servere : Web-serverele, serverele pentru baze de date ;
- *servere de mail* - gestionează mesajele electronice pentru clienţii unei reţele ;
- *servere pentru gestiunea securităţii* - asigură securitatea unei reţele locale cînd aceasta este conectată la o reţea de tipul Internetului. Pot fi incluse în această categorie firewall-urile, proxy serverele ;
- *servere pentru comunicaţii* - asigură schimbul de informaţii între reţea şi clienţii din afara acesteia (accesul prin dial-up, de exemplu).

Pentru desemnarea manierei de proiectare a unei reţele se foloseşte termenul *topologie*. Trebuie să precizăm că există două tipuri de topologii : fizică şi logică. Topologia fizică a unei reţele se referă la configuraţia mediilor de transmisie, a calculatoarelor şi a perifericelor. Topologia logică reprezintă metoda folosită pentru transferul informaţiilor de la un calculator la altul. Despre aceste topologii vom discuta pe larg într-un alt capitol. Pentru moment, facem o scurtă trecere în revistă a topologiilor fizice :

- *bus* (magistrală) ;
- *star* (stea) ;
- *ring* (inel) ;
- *tree* (arbore).

Se cuvine să facem o mică observaţie : această clasificare nu are caracter absolut. Sînt lucrări în care topologia reţelelor este prezentată în altă manieră.

Reţele de tip magistrală (Bus[1])

Topologia magistrală este cea mai simplă modalitate de conectare a calculatoarelor într-o reţea : un singur mediu de transmisie (cablu) la care se conectează toate calculatoarele şi perifericele, denumite în continuare *noduri* (fig. 1.2.1). Fiecare calculator verifică dacă informaţiile pe care le primeşte îi sînt adresate sau nu. Despre acest mecanism vom discuta pe larg într-un alt capitol.

Avantaje	Dezavantaje
Uşurinţă în conectarea calculatoarelor.	Reţeaua nu funcţionează dacă apar întreruperi în cablu.
Necesarul de cablu este redus.	Este nevoie de terminatori la ambele capete ale cablului.
	Problemele sînt greu de identificat dacă reţeaua cade.

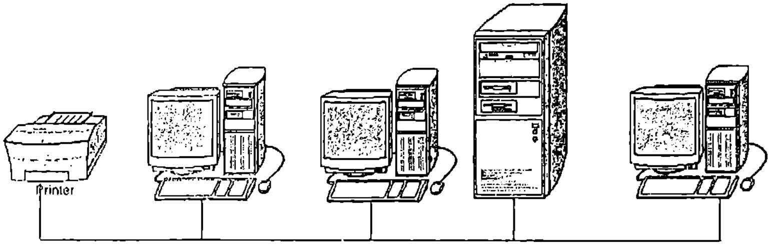


Figura 1.2.1. Topologie de reţea magistrală

Reţele de tip stea (star)

Într-o astfel de reţea, fiecare nod este conectat direct la un *hub* sau *concentrator.*

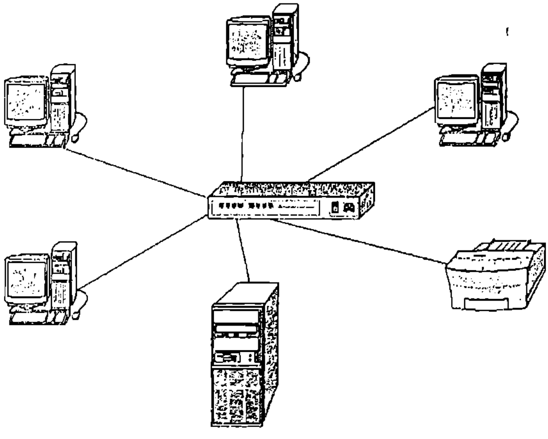


Figura 1.2.2. Topologie de reţea stea

1. A nu se confunda cu *system bus* al calculatorului.

Informaţiile sînt transmise de la calculatorul sursă către cel destinaţie prin intermediul hubu-lui. Acesta este principalul dispozitiv care gestionează şi controlează funcţiile reţelei.

Avantaje	Dezavantaje
Uşurinţă în instalare. Reţeaua nu este afectată dacă sînt adăugate sau retrase calculatoare. Uşurinţă în detectarea problemelor.	Necesită cablu mai mult. Sînt mai costisitoare. Dacă un hub se defectează, toate calculatoarele din acel nod devin nefuncţionabile.

Reţele de tip inel (ring)

Din exterior, o astfel de reţea seamănă foarte mult cu o reţea *star*. Din punctul de vedere al topologiei logice însă, MAU (*Multistation Access Unit*) este dispozitivul care permite informaţiilor să treacă de la un nod la altul în cadrul unui inel comunicaţional.

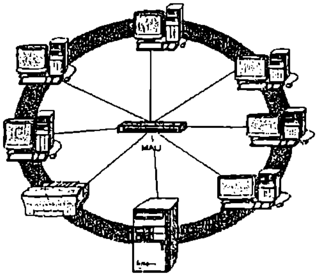


Figura 1.2.3. Topologie de reţea inel

Reţele de tip arbore (tree)

Topologia de reţea *tree* combină caracteristicile topologiilor *bus* şi *star*. Nodurile sînt grupate în mai multe topologii *star* care la rîndul lor sînt legate la un cablu central. Acestea pot fi considerate topologiile cu cea mai bună scalabilitate.

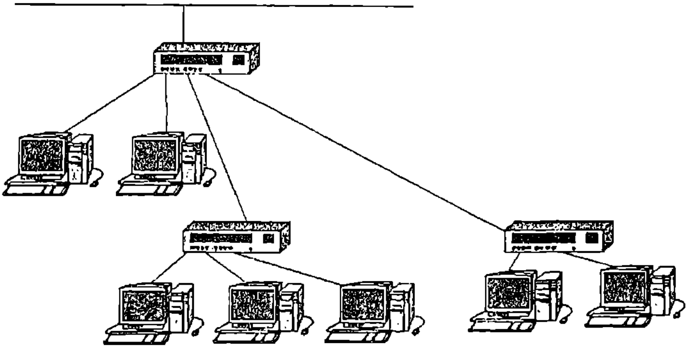


Figura 1.2.4. Topologie de reţea arbore

Avantaje	Dezavantaje
Segmentele individuale au legături directe.	Lungimea maximă a unui segment este limitată. Dacă apar probleme pe conexiunea principală, sînt afectate toate calculatoarele de pe acel segment.

1.2.2. Wide Area Network (WAN – reţele cu . rie mare de întindere)

Pe măsură ce utilizarea calculatoarelor în domeniul economic a devenit omniprezentă, s-a ajuns la concluzia că LAN-urile nu mai corespundeau nevoilor firmelor.

Într-o reţea LAN, fiecare departament era privit ca o „insulă electronică". A apărut însă necesitatea schimbului de informaţii între aceste insule, iar soluţia a reprezentat-o crearea WAN-urilor (Wide Area Network) : reţele care interconectează LAN-uri, furnizînd acces la calculatoare din alte locaţii geografice.

Tehnologiile folosite în cadrul WAN : modem-uri, ISDN (*Integrated Services Digital Network*), DSL (*Digital Subscriber Loop*), Frame Relay, ATM (*Asynchronous Transfer Mode*), T-*Carrier Series* (în SUA T1, T2, T3), SONET (*Synchronous Optical Network*).

1.3. Modelul de referinţă OSI

Conceptul de *nivel* este folosit pentru a ne ajuta să înţelegem acţiunile şi procesele ce apar în timpul transmiterii informaţiilor de la un calculator la altul. Într-o reţea, comunicarea are la origine o sursă, apoi informaţia circulă pînă la o destinaţie. Informaţiile care traversează reţeaua sînt referite ca *date*, *pachete* sau *pachete de date*.

Adresa sursă a unui pachet de date specifică identitatea calculatorului care transmite respectivul pachet. Adresa destinaţie precizează identitatea calculatorului care va recepţiona pachetul. Datele sînt grupate în unităţi logice de informaţii. Ele includ utilizatorul respectivelor informaţii şi alte elemente pe baza cărora este posibilă comunicarea.

Datele dintr-un calculator sînt reprezentate prin biţi. Dacă un calculator ar transmite doar unul sau doi biţi, nu ar fi o manieră prea eficientă de comunicare. Prin urmare, are loc o grupare a acestora în kilo, mega sau gigabytes.

Am făcut deja referire la un alt element întîlnit în reţelele de calculatoare : „mediul". Acesta reprezintă un material prin care sînt transmise datele şi poate fi unul dintre următoarele elemente :

- cablu telefonic ;
- cablu UTP ;
- cablu coaxial (cablu TV) ;
- fibră optică ;
- alte tipuri de cabluri bazate pe cupru.

Mai există şi alte tipuri de media, însă ele nu vor fi luate în calcul în această carte. În primul rînd, este vorba de atmosfera prin care se propagă undele radio, microundele

şi lumina. În al doilea rînd, este vorba de undele electromagnetice care traversează Cosmosul, unde în mod virtual nu există molecule sau atomi. În aceste cazuri, comunicaţia este denumită *fără fir*, iar reţelele sînt de tip wireless.

Protocolul reprezintă un *set de reguli pe baza cărora se determină forma datelor şi transmisia acestora*. Exemplul lui Andrew Tanenbaum[1] (comunicarea între doi filosofi) este un început bun pentru a înţelege ce presupune comunicarea bazată pe niveluri şi protocoale (fig. 1.3.1.).

Nivelul *n* al unui calculator poate comunica cu nivelul *n* al altuia. Prin urmare, se spune că regulile folosite în comunicare se numesc *protocoale de nivel n*.

Un alt exemplu pentru explicarea transferului între două calculatoare este modul în care putem citi o pagină Web aflată pe un calculator situat la mare distanţă :

- utilizatorul lansează un program pentru vizualizarea paginilor Web (browser) ;
- browserul este entitatea aplicaţie care va „negocia" pentru noi obţinerea paginii ;
- nivelul aplicaţie va identifica existenţa resursei cerute de client (clientul este browserul, care-l reprezintă pe utilizator în această „tranzacţie") şi a posesorului acesteia (serverul – înţeles ca fiind entitatea ce oferă resursa cerută, nu calculatorul central al unei reţele ; în cazul nostru, avem de-a face cu un server de Web). Se realizează autentificarea serverului (se verifică dacă partenerul este într-adevăr cine pretinde că este şi se stabileşte dacă acesta este disponibil) ;
- nivelul sesiune va stabili o conexiune între procesul client şi procesul server ;
- nivelul transport se va ocupa de întreţinerea conexiunii şi de corectarea erorilor netratate la nivelul reţea ;
- nivelul reţea va asigura transferul datelor în secvenţe (pachete), stabilind drumul acestora între server şi client.

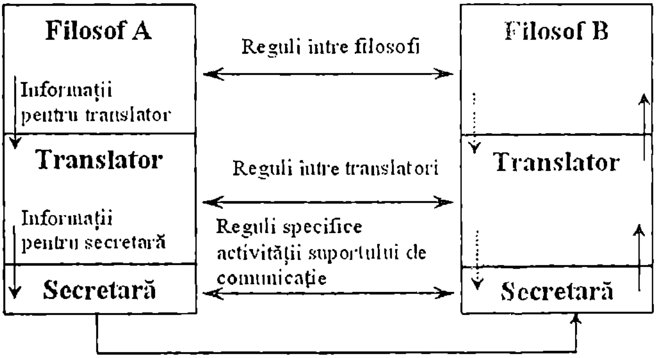


Figura 1.3.1. Modelul de comunicare între filosofi

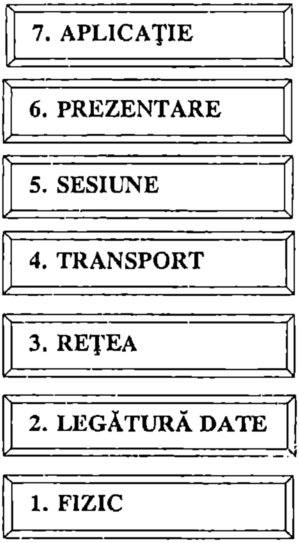
Lucrurile sînt ceva mai complicate decît în cele prezentate mai sus. Datele sosesc prin intermediul mediului de comunicaţie ca un flux de biţi. La nivelul legăturii de date, biţii

1. Adaptare după Andrew S. Tanenbaum : *Reţele de calculatoare*, Ediţia a treia, Editura Agora, Tg. Mureş, 1998, pg. 18.

sînt transformaţi în cadre, iar la nivelul reţea în pachete (vom vedea mai tîrziu cum arată un pachet). În cele din urmă, datele ajung la nivelul aplicaţie unde sînt preluate de browser şi ne sînt prezentate. Fiecare nivel adaugă sau şterge o parte din informaţiile de control ataşate datelor de celelalte niveluri.

Spuneam că dezvoltările timpurii din zona reţelelor au fost haotice şi că începutul anilor '80 se caracterizează printr-o expansiune a acestora. Singura modalitate prin care deţinătorii de reţele puteau să „vorbească aceeaşi limbă" a fost agrearea din partea vînzătorilor şi producătorilor de echipamente de reţea a unui set comun de standarde.

International Organization for Standardization (*ISO*) este organizaţia care a cercetat şi dezvoltat scheme de reţele precum DECNET, SNA, TCP/IP. Rezultatul cercetărilor s-a concretizat într-un model de reţea care i-a ajutat pe producători să creeze echipamente compatibile între ele.



Modelul de referinţă OSI (Open Systems Interconnect), realizat în 1984, nu este altceva decît o schemă descriptivă care a pus la dispoziţia vînzătorilor standardele necesare asigurării compatibilităţii şi interoperabilităţii între diferitele tehnologii. Şi este cel mai bun instrument pentru învăţare.

Modelul de referinţă OSI este primul model pentru standardizarea comunicaţiilor în reţele. Există şi alte modele, dar majoritatea producătorilor de echipamente respectă aceste standarde. Modelul permite utilizatorilor să vadă funcţiile reţelei pe măsură ce ele apar la fiecare nivel în parte. Chiar dacă pare destul de abstract, este un instrument foarte bun pentru a ilustra modul în care informaţiile traversează o reţea: explică vizual circulaţia datelor de la o aplicaţie către mediul fizic de transmisie şi apoi către o altă aplicaţie localizată pe un calculator din reţea, chiar dacă expeditorul şi destinatarul fac parte din reţele cu topologii diferite. După cum se vede şi din figura alăturată, în modelul de referinţă OSI există 7 niveluri, fiecare dintre acestea ilustrînd o funcţie particulară a reţelei. Separarea între funcţiile reţelei este denumită *nivelare* (layering).

Modelul OSI este doar un model de arhitectură de reţea, deoarece spune numai ceea ce ar trebui să facă fiecare nivel, dar nu specifică serviciile şi protocoalele utilizate la fiecare nivel. Fiecare nivel al modelului OSI are un set predeterminat de funcţii pe care le realizează pentru a duce la bun sfîrşit comunicarea.

Nivelul 7: Aplicaţie

Poetic vorbind, este nivelul situat cel mai aproape de inima utilizatorului. Prin ce diferă de celelalte niveluri ale modelului? Oferă servicii pentru aplicaţiile utilizatorilor, dar nu oferă servicii celorlalte niveluri.

Nivelul aplicaţie identifică şi stabileşte disponibilitatea partenerului de comunicaţie, sincronizează aplicaţiile între ele şi stabileşte procedurile pentru controlul integrităţii

datelor şi erorilor. De asemenea, identifică dacă există suficiente resurse pentru a sprijini comunicaţia între parteneri. Pentru a fi mai uşor să vă amintiţi despre acest nivel, gîndiţi-vă la telecomanda TV: o folosiţi, dar nu ştiţi ce se întîmplă în interiorul său.

Nivelul 6: Prezentare

Este nivelul care asigură că informaţiile, pe care nivelul aplicaţie al unui sistem le transmite, pot fi citite de către nivelul aplicaţie al altui sistem. Atunci cînd este necesar, nivelul aplicaţie face translaţie între diferitele formate ale datelor folosind un format comun pentru reprezentarea acestora. Trebuie să priviţi acest nivel ca cel la care are loc codificarea datelor în format ASCII, de exemplu.

Nivelul 5: Sesiune

După cum spune chiar numele său, acest nivel stabileşte, gestionează şi finalizează sesiunile de comunicaţie între aplicaţii. Prin sesiune se înţelege dialogul între două sau mai multe entităţi. Nivelul sesiune sincronizează dialogul între nivelurile sesiune ale entităţilor şi gestionează schimbul de date între acestea. În plus, acest nivel oferă garanţii în ceea ce priveşte expedierea datelor, clase de servicii şi raportarea erorilor. În cîteva cuvinte, acest nivel poate fi asemuit cu dialogul uman.

Nivelul 4: Transport

Este nivelul la care are loc segmentarea şi reasamblarea datelor. El furnizează un serviciu pentru transportul datelor către nivelurile superioare şi, în special, caută să vadă cît de sigur este transportul prin reţea. Nivelul transport oferă mecanisme prin care stabileşte, întreţine şi ordonă închiderea circuitelor virtuale; detectează „căderea" unui transport şi dispune refacerea acestuia; controlează fluxul de date pentru a preveni rescrierea acestora. Gîndiţi-vă la calitatea serviciilor sau la încredere!

Nivelul 3: Reţea

Este unul dintre cele mai complexe niveluri; asigură conectivitatea şi selecţia căilor de comunicaţie între două sisteme ce pot fi localizate în zone geografice diferite. Gîndiţi-vă la selectarea liniilor de cale ferată într-o gară.

Nivelul 2: Legătură date

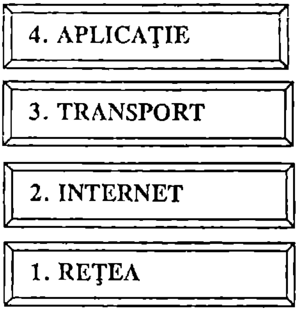
Este nivelul care asigură tranzitarea datelor de la nivelul fizic pe baza adresării fizice, topologiei reţelei, notificării erorilor, ordonarea cadrurilor şi controlul fluxului informaţional. Gîndiţi-vă la controlul accesului pe un aeroport.

Nivelul 1: Fizic

Defineşte specificaţiile electrice, mecanice, procedurale şi funcţionale necesare activării, întreţinerii şi dezactivării legăturii fizice între sisteme. Specificaţiile vizează nivelul voltajului, ratele de transmisie a datelor, distanţa maximă de transmisie, conectorii fizici. Gîndiţi-vă la semnale şi medii de transmisii.

1.4. Modelul TCP/IP

Am început acest capitol cu modelul OSI deoarece reprezintă abecedarul acestui domeniu. Cu toate acestea, pentru transmisiile de date din cea mai mare reţea existentă – Internetul, standardul folosit este *TCP/IP* (*Transport Control Protocol/Internet Protocol*). Acest model a fost creat de Ministerul Apărării din SUA care a dorit să construiască o reţea capabilă să reziste în orice condiţii, chiar şi într-un război nuclear. Era extrem de important să fie creată o reţea capabilă să opereze cu o infrastructură distrusă în proporţie de peste 90%, fără să aibă vreo importanţă starea fizică a anumitor segmente ale reţelei.



Spre deosebire de OSI, modelul TCP/IP are doar patru niveluri: aplicaţie, transport, internet şi reţea. Deşi există două niveluri cu acelaşi nume ca la modelul OSI, nu trebuie confundate cu acelea pentru că fiecare nivel are funcţii total diferite.

Nivelul aplicaţie

Proiectanţii TCP/IP au considerat că protocoalele de nivel înalt din acest model trebuie să includă detalii cu privire la sesiunile de lucru şi modul de prezentare a datelor. Astfel, într-un singur nivel sînt combinate toate facilităţile legate de reprezentarea datelor, codificarea şi controlul dialogului.

Nivelul transport

Acest nivel vizează calitatea serviciilor oferite: încrederea în transmisie, controlul fluxului de date şi corectarea erorilor. Unul dintre protocoalele întîlnite la acest nivel (*Transport Control Protocol*) oferă o modalitate flexibilă de realizare a comunicaţiilor în reţea. Fiind un protocol orientat conexiune, dialogul dintre sursă şi destinaţie se realizează prin împachetarea informaţiilor de la acest nivel în segmente.

Orientarea către conexiune nu înseamnă că între calculatoarele care comunică există vreun circuit, ci că segmentele cu date ale nivelului 4 circulă înainte şi înapoi între cele două calculatoare într-o perioadă de timp dată.

Nivelul internet

Scopul acestui nivel este de a trimite pachetele sursă din orice reţea către o alta şi să facă astfel încît acestea să ajungă la destinaţie indiferent de ruta şi reţeaua din care au fost transmise. Protocolul care guvernează acest nivel este Internet Protocol, funcţiile îndeplinite de acesta fiind determinarea şi comutarea pachetelor (gîndiţi-vă la sistemul poştal).

Nivelul reţea

Numele acestui nivel este cam general şi de multe ori creează confuzie. Este nivelul care include detalii despre tehnologiile LAN/WAN, precum şi toate detaliile incluse în nivelurile fizic şi legătură date din modelul OSI.

De ce trebuie să învăţaţi despre două modele cînd unul (cel mai adesea TCP/IP) ar fi suficient? Specialiştii preferă modelul OSI pentru analize mai atente şi ca fundament în orice discuţie legată de reţele. Este adevărat că TCP/IP este mai folositor pentru că este implementat în lumea reală. Ca utilizatori finali aveţi de-a face numai cu nivelul aplicaţie, dar cunoaşterea detaliată a nivelurilor este vitală pentru realizarea unei reţele. Este adevărat că majoritatea utilizatorilor nu ştiu mai nimic despre protocoalele de rutare sau alte detalii, dar este de asemenea adevărat că aceşti utilizatori nu trebuie să realizeze reţele scalabile şi sigure (şi nici nu au de dat examene la astfel de discipline). Prin urmare, discuţia legată de TCP/IP continuă în capitolele viitoare.

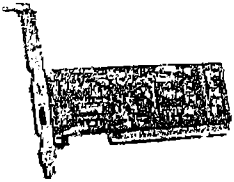
CAPITOLUL 2

Infrastructura rețelei

Clienții, serverele, imprimantele, bazele de date relaționale, dispozitivele de interconectare formează componentele unei rețele locale. Acestea realizează încapsularea și decapsularea datelor pentru a-și îndeplini toate sarcinile (transmitere mail-uri, editare texte, scanare, acces la baze de date). Continuăm prezentarea tehnologiilor prin prisma modelului OSI.

2.1. Cartela de rețea

Ce relație există între o placă de rețea (Network Interface Card) și un computer? NIC este o placă cu circuite ce permite comunicarea în rețea de la și către un computer.



Denumită și *adaptor LAN*, ea se montează într-un *slot* de extensie (PCI) al plăcii de bază avînd un port prin care se realizează conectarea în rețea a computerului.

Similar altor dispozitive hardware, cartela de rețea are nevoie de un *driver* prin care să poată fi controlată. În cazul în care cartela este plug&play, resursele sînt configurate în mod automat simplificîndu-se instalarea. În general, orice cartelă de rețea îndeplinește următoarele funcții:

- pregătește datele pentru a putea fi transmise printr-un mediu;
- transmite datele;
- controlează fluxul datelor de la PC la mediul de transmisie.

Prin rețea datele circulă în serie (un bit o dată), în timp ce în interiorul calculatorului circulă în paralel (16, 32 sau 64 biți o dată, în funcție de bus-ul sistemului). Prin urmare, cartela de rețea trebuie să convertească datele care circulă în interiorul PC-ului în format serial.

Pentru a funcționa, fiecare NIC necesită o întrerupere (IRQ - *Interrupt Request Line*), o adresă I/O și o adresă de memorie. Întreruperea o puteți asocia unei resurse prin care procesorul și celelalte componente ale PC-ului își acordă atenție unele altora. Unele din aceste întreruperi sînt atribuite anumitor dispozitive chiar dacă acestea nu au fost încă instalate fizic în calculator (de exemplu, LPT2 pentru o a doua imprimantă).

În cazul plăcilor de reţea, atribuirea unei întreruperi depinde de numărul întreruperii disponibile pe calculator şi de numărul întreruperii prin care placa de reţea a fost proiectată să acceseze sistemul. Dacă întreruperea pe care este proiectată să lucreze placa de reţea este ocupată de alt dispozitiv, trebuie să rezolvaţi conflictul care apare reconfigurînd cartela să lucreze pe altă întrerupere. Detalii despre toate întreruperile unui PC găsiţi la adresa *http : //www.pcguide.com/ref/mbsys/res/irq*.

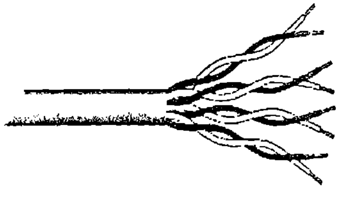
Adresa de memorie (*Memory I/O Address*) va conţine informaţii despre zona de memorie pe care respectivul dispozitiv şi sistemul de operare o vor folosi pentru a-şi transmite date. Intervalul uzual de adrese pe care o placă de reţea îl foloseşte este 0x240-0x360. O parte dintre aceste adrese sînt deja atribuite unor dispozitive. De exemplu, adresa 0x278 este folosită de cel de al doilea port paralel, iar 0x378, de primul. Cartelele de sunet pot folosi 0x220, iar drive-urile CDROM pot folosi 0x300.

2.2. Medii de transmisie

Dacă PC-ul este dotat cu o NIC, nu înseamnă că avem şi o reţea. Ca şi în cazul telefonului, mai este nevoie de un element prin care PC-ul nostru să poată fi legat la reţea. În această categorie intră mediile de transmisie sau cablurile, în limbaj reţelistic. Vom face în continuare o prezentare a principalelor medii de transmisie în funcţie de gradul lor de utilizare în practică.

Unshielded Twisted-Pair (UTP)

Acest mediu de transmisie este format din patru perechi de fire, izolate între ele. Prin torsadarea perechilor de fire apare efectul de anulare, efect ce limitează degradarea semnalelor din cauza interferenţelor magnetice sau radio.



UTP-ul este un cablu uşor de instalat (are un diametru de aproximativ 0,4 cm) şi mult mai ieftin decît alte tipuri de cabluri. Deşi este considerat cel mai rapid mediu de transmisie bazat pe cupru, este mai vulnerabil în faţa zgomotelor electrice în comparaţie cu alte categorii de cabluri.

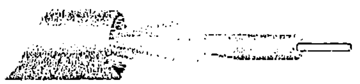
Cablurile UTP din categoria 3 sînt formate din două fire izolate împletite împreună. O variantă mai performantă de astfel de cabluri este categoria 5. Acestea sînt similare celor din categoria 3, dar au mai multe răsuciri pe centimetru şi ar trebui să fie izolate cu teflon, rezultînd de aici o interferenţă redusă şi o mai bună calitate a semnalului pe distanţe mari.

Conectorul standard folosit în cazul acestui cablu este RJ-45 (*Registered Jack*), asemănător cu cel de la firul telefonic. Conectorul este construit în baza unui standard din industria telefonică, standard care precizează care fir trebuie să fie conectat pe un anumit pin al conectorului (vom reveni cu detalii).

Tip cablu	Utilizare
Categoria 1 - 22 sau 24 AWG[1]	Telefonie
Categoria 2 - 22 sau 24 AWG	Transfer date pînă la 4Mbps
Categoria 3 - 24 AWG	Transfer date pînă la 10 Mbps
Categoria 4 - 24 AWG	Transfer date pînă la 20 Mbps
Categoria 5 - 22 sau 24 AWG	Transfer date pînă la 100 Mbps

Fibra optică

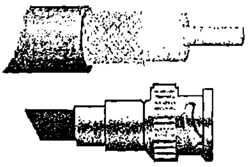
Fibra optică este mediul care asigură transmiterea luminii, modulată la o anumită frecvență. Comparativ cu alte medii de transmisie, fibra optică este cea mai costisitoare, dar nu este susceptibilă la interferențe electromagnetice și, în plus, asigură rate de transfer mult mai ridicate decît celelalte categorii de medii.



Cablul fibră optică constă în două fibre de sticlă îmbrăcate separat într-un înveliș de plastic (materialul se numește Kevlar). Cele două fibre formează inima acestui mediu de transmisie, sticla din care sînt realizate avînd un grad ridicat de refracție. Vom reveni cu mai multe detalii.

Cablul coaxial

Cablul coaxial (coax) constă dintr-un înveliș protector care îmbracă două elemente conductoare: un fir de cupru îmbrăcat într-un material izolator și o folie metalică (sau o plasă) ce acționează ca al doilea fir din circuit. Acest al doilea element este folosit pentru a reduce interferențele externe. Este cablul cu cea mai bună ecranare.



Pentru că nu prea se mai folosește (cu excepția rețelelor „foarte bătrîne"), nu vom mai insista cu alte detalii asupra acestui tip de cablu.

Conectorul folosit de acest tip de cablu se numește BNC (Bayone-Neill-Concelman).

Shielded Twisted-Pair (STP)

Cablul *shielded twisted-pair* (STP) combină trei tehnici legate de transmisia datelor: *shielding* (protejarea), *cancellation* (anularea) și *twisted* (torsadarea) firelor.

Cablul STP de 100 ohm folosit în rețelele Ethernet oferă rezistență atît la interferențele electromagnetice, cît și la cele radio, fără a fi un cablu prea gros.

Învelișul protector folosit în cablul de 150 ohm nu face parte din circuit așa cum se întîmplă în cazul cablului coaxial. Chiar dacă este mai scump decît UTP (*Unshielded Twisted-Pair*), cablul STP oferă protecție împotriva tuturor tipurilor de interferențe. Spre deosebire de cablul coaxial, învelișul protector nu face parte din circuitul electric.

1. *American Wire Gauge Standard.*

O conectare incorectă face ca învelişul protector să acţioneze ca o antenă, absorbind semnalele electrice din cablulrile aflate în vecinătate.

Prin prisma standardelor IEEE 802.3, Ethernetul foloseşte doar cîteva din standardele existente în materie de cabluri : 10Base5, 10Base2, 10BaseT, 10 BaseF, 100BaseF. Notaţia anterioară înseamnă că reţeaua foloseşte o anumită lăţime de bandă, utilizează semnalizarea în banda de bază şi poate suporta segmente de diferite lungimi pe diferite medii de transmisie. Vom face o prezentare sintetizată a acestor standarde.

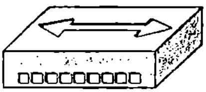
Standard	Mediul fizic	Lăţime de bandă	Lungime segment	Topologie fizică	Topologie logică
10Base2	Coaxial subţire	10Mbps	185 metri	Bus	Bus
10BaseT	UTP categoria 5	10Mbps	100 metri	Star/Extended star	Bus
10BaseFL	Fibră optică multimod	10Mbps	2000 metri	Star	Bus
100BaseTX	UPT categoria 5	100Mbps	100 metri	Star	Bus
100BaseFX	Fibră optică multimod	100Mbps	2000 metri	Star	Bus
1000BaseT	UTP categoria 5	1000Mbps	100 metri	Star	bus

2.3. Echipamente de transmisie a datelor

Chiar dacă acest capitol tratează subiecte legate de nivelul 1 OSI, vom extinde puţin discuţia prezentînd şi echipamentele care corespund nivelurilor 2 şi 3.

Repetorul

Termenul „repetor" vine tocmai de la începuturile comunicării vizuale cînd o persoană aflată pe un deal repeta semnalul pe care tocmai îl primise de la o persoană aflată pe un alt deal situat în vecinătatea sa, pentru a-l transmite mai departe. Telegrafia, telefonia (mai ales cea mobilă) folosesc repetoare de semnal pentru a asigura transmiterea informaţiilor la distanţe foarte mari.

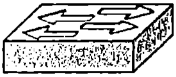


Repetoarele pot fi *single port in - single port out*, *stackable* (modulare) sau *multi port* (cunoscute mai ales sub denumirea de *hub*-uri). Ele sînt clasificate ca fiind componente de nivel 1, deoarece acţionează doar la nivel de biţi. Nu uitaţi : scopul unui hub este de a amplifica şi a retransmite semnale, la nivel de bit, către un număr mai mare de utilizatori : 8,16, sau 24. Procesul prin care se realizează această funcţie se numeşte concentrare.

Fiecare hub are propriul său port prin care se conectează la reţea şi mai multe porturi disponibile pentru calculatoare. Unele hub-uri au un port prin care pot fi legate de o consolă, ceea ce înseamnă că sînt hub-uri gestionabile/cu management. Majoritatea, însă, sînt *dumb hubs* (hub-uri proaste), deoarece doar preiau un semnal din reţea şi îl repetă către fiecare port în parte.

Switch-ul

La prima vedere un switch seamănă foarte bine cu un hub, dar după cum vedeți, simbolul său arată un flux informațional bidirecțional.

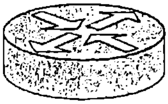


Menirea acestui dispozitiv este de a concentra conectivitatea, garantînd în același timp lățimea de bandă. Switch-ul este un dispozitiv ce combină conectivitatea unui hub cu posibilitatea regularizării traficului pentru fiecare port. Ca manieră de lucru, el comută pachetele de pe porturile transmițătoare către cele destinatare, asigurînd fiecărui port lățimea de bandă maximă a rețelei.

Această comutare a pachetelor se face pe baza adresei MAC, ceea ce face din switch un dispozitiv de nivel 2.

Routerul[1]

Simbolul routerului descrie foarte bine cele două funcții ale sale: selecția căii de transmitere a informațiilor și comutarea pachetelor către cea mai bună rută.



Fizic, routerele se prezintă sub o mulțime de forme, în funcție de model și de producător. Componentele principale ale routerului sînt interfețele prin care rețeaua proprietară se conectează la alte segmente de rețea. Din acest motiv el este considerat un dispozitiv inter-rețele.

Scopul routerului este să examineze pachetele recepționate, să aleagă cea mai bună cale de transmitere a acestora și, în final, să le transfere către portul corespunzător. Pentru rețelele mari, el reprezintă cel mai important dispozitiv prin care se reglează traficul rețelei. Deciziile routerului, în ceea ce privește selectarea căii de rutare, se iau pe baza informațiilor de la nivelul 3 (adresele de rețea), motiv pentru care sînt considerate echipamente de nivel 3. De asemenea, ele asigură conectivitate pentru diferitele tehnologii ale nivelului 2: Ethernet, Token Ring, FDDI.

În concluzie:

Echipament	Nivelul OSI la care lucrează	Protocol	Domeniu	Cu ce lucrează
Repetoare/hub-uri	1	Transparent	Amplifică semnalul	Biți
Bridge	2	Transparent	Domeniu de coliziune	Cadre
Switch	2	Transparent	Domeniu de coliziune	Cadre
Router	3	Dedicat	Domeniu de broadcast	Pachete

Dacă lucrurile nu sînt prea clare încă, încercați să citiți și materialele de la următoarele adrese:

- http://www.whatis.com/encapsul.htm,
- http://www.jyu.fi/,
- http://www.cs.mun.ca/,
- http://www.erg.abdn.ac.uk/users/gorry/course/intro-pages/encapsulation.html.

1. În unele lucrări de la noi este denumit și repartitor.

CAPITOLUL 3

Nivelul legătură date

Pînă în acest moment am discutat mai mult despre ce se întîmplă la nivel fizic într-o rețea: medii de transmisie, biții care traversează aceste medii, componente care transmit semnale electrice și topologii. Nivelul 1 joacă un rol important în comunicația dintre calculatoare, dar efortul său singular nu este de ajuns. Fiecare dintre funcțiile nivelului 1 are propriile limitări, dar acestea sînt eliminate prin ceea ce se întîmplă la nivelul 2.

The Institute of Electrical and Electronic Engineers (IEEE)[1] este organizația profesională care a definit standardele aplicabile în domeniul rețelelor de calculatoare:

- 802.1- modul de interconectare în rețea;
- 802.2- controlul legăturii logice (LLC);
- 802.3- rețele LAN cu acces multiplu și cu detectarea purtătoarei și a coliziunilor CSMA / CD, sau **rețelele Ethernet**[2];
- 802.4- rețele LAN cu transfer de jeton pe magistrală (Token Bus);
- 802.5- rețele LAN cu transfer de jeton în inel (Token Ring);
- 802.6- rețele metropolitane (MAN);
- 802.11- rețele fără fir;
- 802.12-rețele LAN cu prioritate la cerere.

Conform standardului Ethernet, o rețea locală este compusă din noduri și medii de interconectare. Nodurile pot fi împărțite în două categorii:

- **Data terminal equipment (DTE)** – sînt echipamentele care funcționează ca sursă sau destinație a cadrelor transmise prin rețea. Cel mai adesea, în această categorie intră PC-urile.
- **Data communication equipment (DCE)** – sînt dispozitive intermediare care recepționează și transmit cadrele prin rețea. Se includ în această categorie hub-urile, switch-urile, routerele, NIC-urile sau modem-urile.

În timp ce modelul OSI reprezintă teoria care a stat la baza dezvoltării rețelelor, standardele IEEE au apărut în momentul în care rețelele au devenit realitate, cînd problemele practice trebuiau rezolvate. Chiar dacă modelul OSI este folosit în continuare,

1. http://standards.ieee.org.
2. Pe larg la adresa http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ethernet.htm.

cînd se vorbeşte de nivelul 2, se au în vedere şi cele două noi componente apărute în timp : LLC şi MAC :

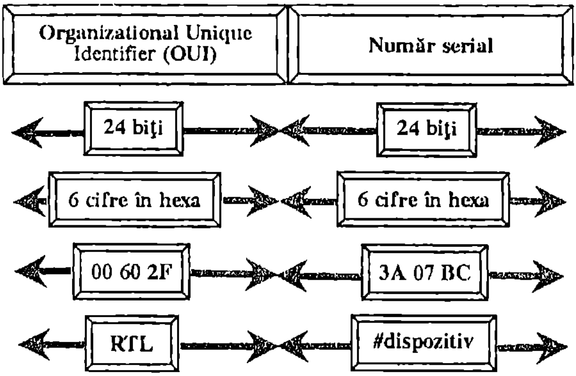
- **Media Access Control** (MAC) - realizează tranziţia în jos, către mediul fizic de transmisie.
- **Logical Link Control** (LLC)[1] - realizează tranziţia în sus, către nivelul reţea.

Subnivelul LLC este independent de tehnologia folosită, în timp ce MAC este dependent de tehnologia folosită.

3.1. Funcţiile MAC

Subnivelul LLC a fost introdus de către IEEE din nevoia de a asigura independenţa tehnologică a unora dintre funcţiile nivelului legătură date. Oarecum inconsistent în serviciile pe care le oferă protocoalelor de la nivelul reţea, subnivelul LLC comunică cu tehnologiile specifice nivelurilor dinaintea sa.

LLC preia datele protocolului reţea şi le adaugă mai multe informaţii de control pentru a transmite pachetele IP către destinaţie. Pachetul IP astfel reîmpachetat este transmis subnivelului MAC unde urmează a fi încapsulat.



Subnivelul LLC răspunde de gestionarea comunicaţiilor între echipamentele de pe o singură linie/legătură a reţelei. LLC este definit prin specificaţiile IEEE 802.2, specificaţii care se referă atît la serviciile orientate conexiune, cît şi la cele fără conexiune, servicii folosite de protocoalele superioare.

Subnivelul MAC se ocupă de protocoalele pe care un calculator le foloseşte pentru a accesa mediul fizic de transmisie a datelor. Adresa MAC are o lungime de 48 de biţi şi este exprimată în hexazecimal (12 cifre). Primele 6 care formează OUI (*Organizational Unique Identifier*) sînt administrate de către IEEE, identificînd producătorul sau vînzătorul

1. Definit prin IEEE 802.2.

produsului. Celelalte 6 descriu numărul interfeței (*Serial Number Interface*) sau o altă valoare administrată de fiecare producător sau vînzător.

Adresa MAC este „scrisă" în memoria ROM a cartelei de rețea, de unde este apoi copiată în RAM la inițializarea cartelei. Prin urmare, dacă o cartelă este înlocuită, se va schimba și adresa fizică a calculatorului.

Cînd un dispozitiv din cadrul unei rețele Ethernet încearcă să transmită date către alt dispozitiv, va căuta să deschidă un canal de comunicație cu acesta, folosind adresa MAC : datele transmise vor transporta și adresa MAC a destinației. Pe măsură ce datele traversează mediul fizic de transmisie, NIC-ul fiecărui calculator din rețea verifică dacă adresa sa MAC corespunde adresei destinație incluse în pachet. Dacă adresele nu sînt identice, NIC ignoră datele din pachet, date ce continuă să circule către următoarea destinație. Dacă adresele sînt identice, NIC face o copie a pachetului cu date și plasează această copie în calculator, la nivelul legătură de date. Pachetul original va continua să circule prin rețea, către alte destinații, unde se va verifica corespondența dintre adresele MAC.

Dezavantajul major al adresării MAC constă în faptul că aceste adrese nu au o structură strict definită : vînzătorii au OUI-uri diferite. Altfel spus, adresarea MAC nu este o adresare ierarhică, după cum se va vedea că este adresarea IP. Pe măsură ce rețeaua „crește", acest dezavantaj devine o problemă majoră. Nu uitați : de fiecare dată cînd se discută de adresa MAC, trebuie să vă gîndiți la nivelul legătură date.

3.2. Încadrarea (*framing*) și standardul Ethernet

Framing-ul sau *încadrarea* este un mecanism prin care se obțin informații complexe, operație ce nu poate fi realizată prin simpla transmisie a biților prin mediul fizic al rețelei. Care sînt calculatoarele ce doresc să comunice între ele ? Cînd începe comunicarea între două calculatoare și cînd se termină ? Cînd îi vine rîndul unui calculator să comunice ?

Spuneam că nivelul fizic al unui calculator se ocupă doar de biți. În timp ce încearcă să transmită acești biți către destinație, nivelul fizic nu garantează că nu există și erori. Aici intervine nivelul legătură date. Prin încadrare, biții transmiși de nivelul fizic sînt încapsulați la nivelul 2 în unități de date ale protocolului de nivel 2 (PDU de nivel 2) sau cadre (*frame*-uri).

Există mai multe tipuri de cadre, în funcție de standardele folosite la descrierea lor. Standardul Ethernet este definit de IEEE (*Institute for Electrical and Electronic Engineers*) ca IEEE 802.3. Acest standard definește regulile pentru configurarea unei rețele Ethernet precum și modul de interacțiune între diferitele elemente ale unei astfel de rețele (există 18 variante ale acestui standard !).

În mod generic, un cadru este împărțit în secțiuni numite cîmpuri, fiecare cîmp fiind alcătuit din *bytes* :

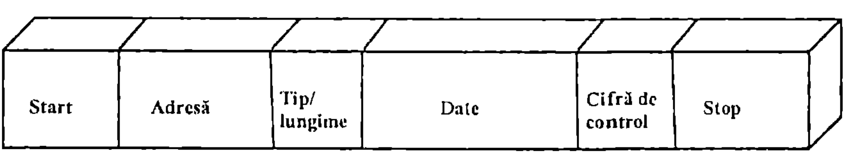


Figura 3.2.1. Structura generală a unui cadru

Orice calculator conectat la o reţea trebuie să deţină un mecanism prin care să poată atrage atenţia celorlalte calculatoare din reţea cu privire la transmiterea unui cadru. Acest lucru este posibil prin intermediul cîmpului *start* din formatul cadrului.

Orice cadru conţine informaţii cu privire la numele calculatorului sursă (sub forma adresei MAC) şi numele calculatorului destinaţie (tot adresa MAC). Un cadru are însă şi cîmpuri specializate: lungimea exactă a cadrului sau tipul său, pentru a specifica protocolul de nivel 3 ce face posibilă transmiterea sa prin reţea.

Datele transmise prin reţea sînt împărţite în două componente: datele propriu-zise şi un set de bytes încapsulaţi, denumiţi *padding bytes* sau *bytes de umplere*. Aceşti bytes sînt adăugaţi cadrului pentru ca acesta să aibă o lungime minimă şi să poată respecta intervalul de timp în care este transmis.

Informaţiile conţinute de un cadru sînt susceptibile de a suporta erori ce pot să aibă surse diferite. Cadrele care conţin erori sînt retransmise. Acest lucru este realizat cu ajutorul cîmpului secvenţă/cifră de control al cadrului. Această cifră este un număr obţinut pe baza datelor din cîmpul de date al cadrului. Cifra de control este citită de calculatorul destinaţie pentru a verifica în ce măsură cadrul recepţionat este corect sau este alterat de zgomotele reţelei.

Calculatorul sursă calculează o cifră de control pe care o adaugă cadrului. La destinaţie, se calculează o nouă cifră de control pe baza datelor conţinute de cadrul recepţionat, cifră care este comparată cu cea calculată de sursa mesajului. Dacă cele două cifre de control sînt identice, datele din cadru vor fi acceptate. În situaţia în care cifrele de control nu sînt identice, sursa va fi atenţionată că trebuie să retransmită datele. Pentru ca transmisia să se termine în condiţii optime, sursa mesajului trebuie să atragă atenţia celorlalte calculatoare asupra momentului în care cadrul se termină.

3.2.1. Cadrul Ethernet[1]

Fiecare calculator echipat cu o placă de reţea Ethernet funcţionează independent de toate celelalte staţii din reţea: nu există un control centralizat. Toate staţiile ataşate la reţea sînt conectate la acelaşi sistem de transport pentru semnal, denumit mediu de comunicaţie. Informaţia este transmisă serial, bit cu bit prin linia de comunicaţie către toate staţiile ataşate acesteia. Figura următoare ilustrează formatul unui cadru Ethernet aşa cum este el prezentat în specificaţiile IEEE 802.3[2] (cifrele reprezintă lungimea cîmpurilor în bytes).

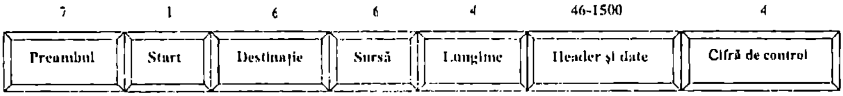


Figura 3.2.2. Structura cadrului Ethernet

Conform acestui standard, cîmpurile care alcătuiesc un cadru Ethernet sînt:

1. Vezi detalii la http://www.ethermanage.com/ethernet/ethernet.html.
2. http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ethernet.htm#xtocid8.

- *Preambul*

Această secvență de 56 biți este folosită pentru sincronizarea transmisiei. Acești biți permit componentelor unei rețele să detecteze prezența unui semnal și să înceapă citirea acestui semnal înainte de sosirea datelor conținute în cadrul respectiv. Prin intermediul acestor biți, stația destinatară este avertizată cu privire la sosirea unui cadru.

- *Start cadru*

Conform specificațiilor IEEE 802.3, byte-ul care delimitează începutul cadrului de restul conținutului său se termină cu doi biți consecutivi cu valoarea 1 (10101011). Acești biți servesc la sincronizarea recepției cadrului de către toate stațiile.

- *Adresă destinație și adresă sursă*

Primii 3 bytes ai acestui cîmp sînt precizați de către IEEE în funcție de cerințele producătorilor de echipamente pentru rețele. Următorii 3 sînt descriși chiar de producători. Adresa sursă este o adresă unicast (*single node*). Adresa destinație poate fi unicast (un singur calculator), multicast (mai multe calculatoare) sau broadcast (toate calculatoarele).

- *Lungime/tip*

Acest cîmp indică numărul de bytes de date care urmează în cadru după acest cîmp sau tipul cadrului, dacă acesta este asamblat folosind un format opțional.

- *Date*

După ce procesările de la nivelurile fizic și legătură date s-au terminat, datele conținute în cadru sînt transmise către un protocol de nivel superior, care trebuie definit în cadrul acestui cîmp. Dacă datele din cadru nu ocupă cel puțin 46 bytes, vor fi inserați bytes de umplere pînă la atingerea acestei valori.

- *Cifră de control*

Acest cîmp conține o cifră de verificare pe 4 bytes, cifră ce este calculată de către dispozitivul care transmite datele, urmînd a fi recalculată de către receptor și comparată cu originalul în scopul identificării eventualelor diferențe.

Dispozitivele Ethernet trebuie să permită un interval minim de timp între două cadre care se transmit pe un mediu. Acest interval se numește *interframe gap (IFG)* sau *interpacket gap (IPG)* și folosește pentru pregătirea recepționării următorului cadru transmis de o stație. Acest interval este de 9,6 microsecunde pentru rețelele pe 10 Mbps, 960 nanosecunde pentru 100 Mbps și 96 nanosecunde pentru 1 Gbps.

În continuare vom prezenta cele două protocoale prin care se controlează accesul la mediul de transmisie într-o rețea Ethernet: *half-duplex* și *full-duplex*.

3.2.2. Half-Duplex Ethernet[1] (CSMA/CD Access Protocol)

Half Duplexul reprezintă forma tradițională de control în Ethernet, bazată pe protocolul CSMA/CD - Carrier Sense Multiple Access/Collision Detection (acces multiplu cu detecția purtătoarei și coliziunii).

1. Comunicație semi-duplex.

Pe baza acestui protocol, staţiile care partajează acelaşi mediu şi care doresc să iniţieze o transmisie trebuie să asculte canalul pentru a vedea dacă nu cumva transmite altcineva în acel moment. În cazul în care canalul este ocupat, staţia aşteaptă pînă la eliberarea acestuia. Atunci cînd canalul este liber, staţia transmite un cadru către toate celelalte staţii (operaţie care se numeşte *broadcast* sau *difuzare)*. Există însă probabilitatea ca, imediat ce această staţie începe să transmită, o altă staţie să fie pregătită de transmisie şi să asculte canalul. În situaţia în care cadrul difuzat în reţea nu a ajuns încă la cea de a doua staţie, aceasta din urmă va detecta canalul ca fiind liber şi va iniţia, la rîndul său, o transmisie, rezultînd o coliziune.

Coliziunile pot fi detectate urmărind puterea sau lăţimea impulsului semnalului recepţionat şi comparîndu-le cu semnalul transmis. În acest caz, staţia care a iniţiat transmisia lansează în reţea o secvenţă *jam* (de blocare) de 32 biţi prin care se asigură că toate celelalte staţii din reţea au fost informate cu privire la eşuarea transmisiei. Apoi, staţia sursă îşi abandonează transmisia, aşteaptă o perioadă de timp şi încearcă iarăşi, dacă nici o altă staţie nu a început să transmită intre timp. Acest proces se repetă pînă cînd cadrul este transmis cu succes la destinaţie.

În sinteză, principalele etape în transmiterea unui cadru sînt:

1. staţia care doreşte să transmită ascultă reţeaua cu scopul detectării prezenţei unei staţii care transmite (*carrier sense* – detecţia purtătoarei);
2. dacă este detectată o purtătoare activă, transmisia este amînată. Staţia continuă să monitorizeze reţeaua pînă în momentul dispariţiei purtătoarei;
3. dacă nu este detectată o purtătoare activă, staţia sursă iniţiază transmiterea cadrelor;
4. o dată cu transmiterea cadrului, staţia sursă supraveghează mediul în vederea detectării coliziunilor;
5. dacă este detectată o coliziune, staţia sursă opreşte transmisia cadrelor şi lansează o secvenţă de blocare pentru a se asigura că toate celelalte staţii iau cunoştinţă de existenţa coliziunii;
6. după ce a transmis secvenţa de blocare, staţia sursă aşteaptă o perioadă de timp înainte de a reîncepe transmisia (de la punctul 1). Acest proces se numeşte *backoff algorithm*[1] (algoritm de regresie): se reduce probabilitatea de apariţie a coliziunilor prin adaptarea dinamică a numărului staţiilor care încearcă să transmită (interval de întîrziere generat aleatoriu);
7. dacă totuşi reapar coliziuni, intervalul de generare aleatorie creşte exponenţial. Algoritmul asigură o întîrziere minimă cînd se „ciocnesc" numai cîteva staţii, dar garantează că ciocnirea este rezolvată într-un interval rezonabil cînd este vorba de mai multe staţii;
8. procesul se repetă pînă cînd o staţie transmite un cadru fără coliziuni.

Un parametru important al operării în modul half duplex este *slot time* (mărimea cuantei). Acest parametru a fost definit ca avînd 512 intervale de bit (51,2 microsecunde) pentru reţelele Ethernet care operează la viteze de 10 şi 100 Mbps, respectiv 4096

1. *Binary exponential backoff algorithm* (algoritm de regresie binară exponenţială). Pentru detalii, vezi A. Tanenbaum, *Reţele de calculatoare*, Ed. Agora 1998.

intervale de bit pentru rețelele Gigabit. Mărimea cuantei se referă la intervalul de timp pe care un dispozitiv îl așteaptă înainte de a retransmite după apariția unei coliziuni.

Pe măsură ce traversează rețeaua, semnalele transmise suferă întîrzieri. Aceste întîrzieri reprezintă timpul necesar unui semnal să tranziteze prin componentele electronice ale rețelei. Cu cît lungimea segmentelor și numărul de repetoare (hub-uri) se apropie de maximul admis de standardele Ethernet (2500 metri și 4 repetoare), cu atît se mărește și intervalul de timp necesar unui semnal pentru a traversa rețeaua de la un capăt la altul. Acest interval de timp se numește *întîrziere la propagare*.

Suma dintre întîrzierea dus-întors la propagare (maximă) și timpul necesar pentru a transmite o secvență de blocare sînt componentele care definesc mărimea cuantei în Ethernet.

O cuantă cu mărimea de 512 intervale de bit stabilește mărimea minimă a unui cadru Ethernet la 64 bytes (în cazul Gigabyte, cele 4096 intervale de bit impun adăugarea unui cîmp de extensie la cadru pentru a se atinge mărimea minimă de 512 bytes). Orice cadru a cărui dimensiune este mai mică de 64 bytes este considerat *fragment de coliziune* și este distrus în mod automat de stația care îl recepționează.

Mărimea cuantei impune o limită maximă în ceea ce privește dimensiunea unei rețele: lungimea segmentelor de cablu și numărul repetoarelor pe o singură cale. Dacă rețeaua este dezvoltată dincolo de aceste limite, apare fenomenul de *coliziune întîrziată*. Acestea sînt coliziunile care apar prea tîrziu în timpul transmiterii unui cadru pentru a mai putea fi gestionate prin funcția de control al accesului. Cadrele afectate vor fi distruse, fiind necesară reinițierea transmisiei.

Mărimea cuantei este cea care asigură că aceasta va fi identificată în primii 512 biți transmiși sub formă de cadre, dacă este posibil să apară o coliziune.

Revenim acum la algoritmul de regresie pentru a explica mai în detaliu ce se întîmplă. Prin intermediul acestui algoritm stația care a inițiat transmisia determină intervalul de timp care trebuie să treacă după apariția unei coliziuni, înainte ca un cadru să fie retransmis. De ce este nevoie de așa ceva? Dacă toate stațiile ar aștepta același interval de timp, atunci în mod sigur va apărea o nouă coliziune. Acest lucru este evitat prin algoritmul amintit: fiecare stație generează aleator un număr care va determina timpul cît trebuie să aștepte înainte de a trece la identificarea purtătoarei. Acest interval de timp se numește *întîrziere de regresie*.

După apariția primei coliziuni, fiecare stație așteaptă 0 sau 1 cuante înainte de a încerca o nouă transmisie. Dacă apare o nouă coliziune, intervalul de așteptare va fi între 0 și 3 cuante, pentru o a treia coliziune, între 0 și 7 (2^3-1). În general, după *i* coliziuni se așteaptă între 0 și 2^i-1 cuante. Dacă se ajunge la un număr de 10 coliziuni, intervalul de așteptare este înghețat la 1023 cuante. După 16 coliziuni, funcția MAC raportează eșecul calculatorului (**excessive collision error**), iar cadrul care trebuia transmis este distrus, aplicația care îl folosea fiind nevoită să inițieze o nouă transmisie.

De ce atîtea vorbe despre acest algoritm? Pentru că erorile care apar ca urmare a coliziunilor în exces dintr-o rețea reprezintă cel mai bun indiciu că rețeaua nu mai este eficientă.

Timpul necesar transmiterii unui cadru este invers proporțional cu rata de transmisie. Pentru o rețea cu o lățime de bandă de 100Mbps, un cadru cu o dimensiune minimă este transmis într-un timp egal cu 1/10 din mărimea cuantei. Prin urmare, o coliziune care apare în timpul acestei transmisii nu va putea fi detectată de stațiile care emit semnal.

Este motivul pentru care diametrul maxim al unei reţele pe 10 Mbps nu poate fi utilizat în cazul reţelelor pe 100Mbps (Fast Ethernet). Soluţia în acest caz a fost reducerea diametrului reţei.

Parametru	10 Mbps	100 Mbps	1000 Mbps
Mărimea minimă a unui cadru	64 bytes	64 bytes	520 bytes
Diametrul maxim al domeniului de coliziune	100 metri UTP	100 metri UTP 412 metri fibră optică	100 metri UTP 316 metri fibră optică
Diametrul maxim al domeniului de coliziune cînd se folosesc repetoare	2500 metri	205 metri	200 metri
Numărul maxim de repetoare pe o rută LAN	5	2	1

3.2.3. Full-Duplex Ethernet[1]

Cel de-al doilea mod de operare al reţelelor Ethernet depăşeşte limitările impuse prin protocolul CSMA/CD : o staţie, la un moment dat, poate fie să transmită date, fie să le recepţioneze. Niciodată nu se întîmplă acest lucru simultan.

În cazul full-duplex-ului, două staţii pot să schimbe simultan informaţii, dacă există o legătură care să permită acest lucru. În acest caz, *throughput*-ul agregat al reţelei se dublează !

Operarea în modul full-duplex este restricţionată de respectarea mai multor criterii. În primul rînd, mediul fizic de transmisie trebuie să suporte transmiterea şi recepţionarea simultană de informaţii, fără a exista interferenţe. Mediile ale căror specificaţii *respectă* aceste cerinţe sînt : 10-Base-T, 10Base-FL, 100Base-TX, 100Base-FX, 100Base-T2, 1000Base-CX, 1000Base-SX, 1000Base-LS şi 1000Base-T. Următoarele specificaţii *nu* suportă modul full-duplex : 10Base5, 10Base2, 10Base-FP, 10Base-FB, 100Base-T4.

În al doilea rînd, pentru a opera în acest mod, legăturile trebuie să fie *point-to-point* (punct-la-punct) sau, altfel spus, legătura trebuie să fie direct între două staţii. Atît timp cît nu există conflicte ca în cazul mediilor partajate, nu vor apărea coliziuni şi, prin urmare, nici protocolul CSMA/CD nu mai este necesar. Ambele staţii trebuie să suporte şi să fie configurate pentru a opera în modul full-duplex.

Deşi mai sînt destule de spus, ne oprim aici cu descrierea Ethernetului nu înainte de a mai aminti despre *agregarea legăturii* sau *trunking*-ul disponibil în modul full-duplex. Acest lucru înseamnă că mai multe legături fizice de tip point-to-point pot fi agregate pentru a funcţiona ca o singură legătură logică.

În concluzie, nivelul legătură date îndeplineşte următoarele funcţii :

- arbitrare : determină dacă se poate folosi mediul fizic de transmisie a datelor ;
- adresare : asigură că datele au fost recepţionate şi procesate de către destinatarul corect ;
- detectarea erorilor : determină dacă datele au ajuns la destinaţie nealterate.

1. Duplex integral.

3.3. FDDI[1]

Comitetul de standardizare ANSI X3T9.5 este primul autor al standardului **Fiber Distributed Data Interface (FDDI)**. După completarea tuturor specificaţiilor, ANSI a transmis standardul FDDI Organizaţiei Internaţionale pentru Standardizare (ISO) care a realizat o versiune internaţională a standardului FDDI, versiune perfect compatibilă cu versiunea ANSI. Chiar dacă astăzi reţelele FDDI nu sînt atît de comune precum cele Ethernet, pe măsură ce costurile de implementare se vor reduce, ele vor deveni accesibile pe o scară mai mare.

FDDI prezintă 4 specificaţii :

Media Access Control (MAC) - defineşte modul în care se realizează accesul la mediul fizic de transmisie, incluzînd : formatul cadrului, adresarea, manipularea jetonului, algoritmul prin care se calculează CRC (verificarea redundanţei ciclice) şi mecanismele pentru refacerea stării iniţiale ca urmare a apariţiei unei erori.

Physical Layer Protocol - protocolul nivelului fizic defineşte procedurile pentru codificarea/decodificarea datelor, incluzînd : cerinţele ceasului (frecvenţa), încadrarea şi alte funcţii.

Physical Layer Medium - mediul nivelului fizic defineşte caracteristicile mediului de transmisie, incluzînd : conexiunile fibrei optice, ratele de eroare la nivel de bit, componentele optice.

Station Management - defineşte configuraţia staţiilor într-o reţea FDDI, incluzînd : configuraţia inelului, adăugarea şi eliminarea staţiilor, iniţializarea, izolarea căderilor, statistici.

După cum se vede şi din figura următoare, cîmpurile ce alcătuiesc un cadru FDDI sînt :

- *Preambul* - pregăteşte fiecare staţie pentru a putea recepţiona cadrul.
- *Delimitator de start* - indică începutul unui cadru.
- *Control* - indică mărimea cîmpurilor adresă şi conţine informaţii de control (de exemplu, dacă datele sînt asincrone sau sincrone).

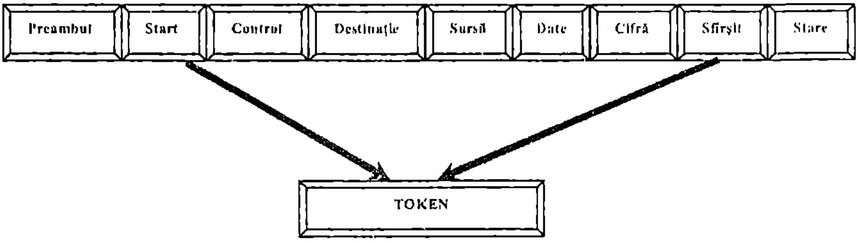


Figura 3.3.1. Structura cadrului FDDI

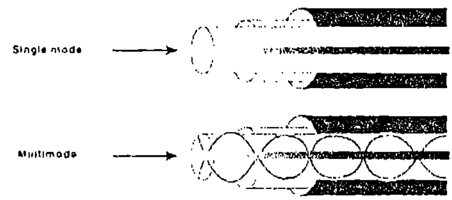
- *Adresă destinaţie* - conţine o singură adresă (unicast), un grup de adrese (multicast) sau adresele tuturor staţiilor (broadcast). Adresele au 6 bytes.

1. Vezi şi http://www.ieng.com/univercd/cc/td/doc/cisintwk/ito_doc/fddi.htm.

- *Adresă sursă* - identifică staţia care trimite cadrul (are 6 bytes).
- *Date* - conţine informaţii de control sau informaţii destinate unui protocol de nivel superior.
- *Cifră de control* - este completată de staţia sursă care calculează o CRC. Această valoare depinde de conţinutul cadrului. Staţia destinaţie recalculează această valoare pentru a determina dacă a fost modificat cadrul în timpul tranzitării prin reţea.
- *Delimitator de sfîrşit* - indică sfîrşitul cadrului.
- *Stare* - permite staţiei sursă să determine apariţia erorilor şi dacă la destinaţie cadrul a fost recepţionat şi copiat de respectiva staţie.

Strategia folosită în reţelele FDDI pentru transmiterea jetonului este similară cu cea din reţelele token-ring. FDDI permite alocarea lăţimii de bandă în timp real, fapt ce le face ideale pentru o mare varietate de aplicaţii. Acest lucru este posibil prin cele două tipuri de trafic ce pot fi implementate: sincron şi asincron.

Traficul sincron poate consuma doar o porţiune din totalul lăţimii de bandă a unei reţele (să zicem 100Mbps), în timp ce traficul asincron consumă restul. Lăţimea de bandă pentru traficul sincron este alocată staţiilor care necesită transmiterea continuă a datelor (de exemplu, voce sau video). Specificaţiile FDDI SMT definesc o schemă distribuită prin care se alocă lăţimea de bandă.



În traficul asincron, lăţimea de bandă este alocată folosind o schemă de priorităţi pe opt niveluri. Fiecare staţie are atribuit un nivel de prioritate asincron şi poate folosi la un moment dat toată lăţimea de bandă asincronă. Mecanismul de prioritate poate bloca staţiile care nu folosesc lăţimea de bandă sau care au un nivel de prioritate prea mic.

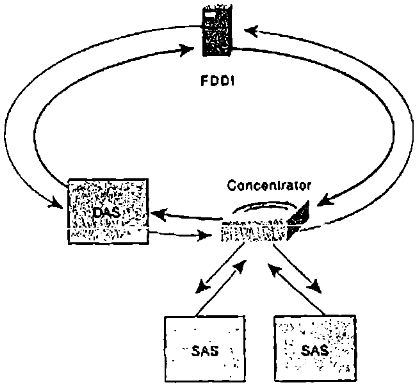
Specificaţiile FDDI definesc două tipuri de fibră: *single mod* (sau mono-mod) şi *multi mod*. Aceste moduri se referă la fascicolul de lumină care intră în fibra optică sub un anumit unghi.

Mono-modul, după cum îi spune şi numele, permite unui singur tip de fascicol să se propage prin fibră, în timp ce multi-modul suportă mai multe tipuri de fascicole. Deoarece în multi-mod lumina care se propagă prin fibră poate parcurge distanţe diferite (în funcţie de unghiul de incidenţă), iar semnalele pot să ajungă la destinaţie la intervale diferite de timp, mono-modul oferă lăţime de bandă mai mare. Acesta este şi motivul pentru care fibra mono-mod este folosită mai ales la cablările între clădiri în timp ce fibra multi-mod se foloseşte pentru cablările intra-clădiri.

Dispozitivele prin care se generează lumină sînt LED-urile pentru fibra multi-mod şi laserul pentru fibra mono-mod.

Conform specificaţiilor FDDI, pentru realizarea conexiunilor fizice se foloseşte un inel (*ring*) dublu. Prin fiecare dintre aceste inele, traficul se desfăşoară în sensuri opuse. Fizic, inelele sînt alcătuite din două sau mai multe conexiuni punct-la-punct între staţiile adiacente. Unul dintre cele două inele se numeşte inel principal şi este folosit pentru transmiterea datelor. Cel de-al doilea inel se numeşte secundar şi este folosit, în general, pentru back-up.

În FDDI se întîlnesc două categorii de staţii:



Single Attachement Stations (SAS) sau stații din clasa B, atașate inelului principal prin intermediul unui concentrator care oferă conectivitate pentru mai multe astfel de stații și asigură continuitatea rețelei în cazul întreruperilor de tensiune sau „căderilor" oricăreia dintre stații.

Dual Attachement Stations (DAS) sau stații din clasa A atașate ambelor inele. Fiecare dintre aceste stații are două porturi (A și B) prin care se conectează la ambele inele ale FDDI.

3.4. Domenii de coliziune

Coliziunea apare în momentul în care biții transmiși de două calculatoare se întîlnesc pe același mediu de transmisie. Fizic, în cazul cablurilor bazate pe cupru acest lucru înseamnă un plus de voltaj în respectivul mediu, lucru care nu este permis în sistemele binare care sînt capabile să *înțeleagă* doar două valori ale voltajului.

Majoritatea tehnologiilor de rețea se confruntă cu această problemă. În unele cazuri, coliziunile sînt parte componentă a rețelei. Prea multe coliziuni însă pot conduce la încetinirea rețelei sau chiar la întreruperea funcționării acesteia. Dacă există reguli în baza cărora această problemă să poată fi controlată, lucrurile nu sînt deloc complicate.

Rețelele Ethernet folosesc mecanismul CSMA/CD prin care identifică coliziunile apărute la un moment dat.

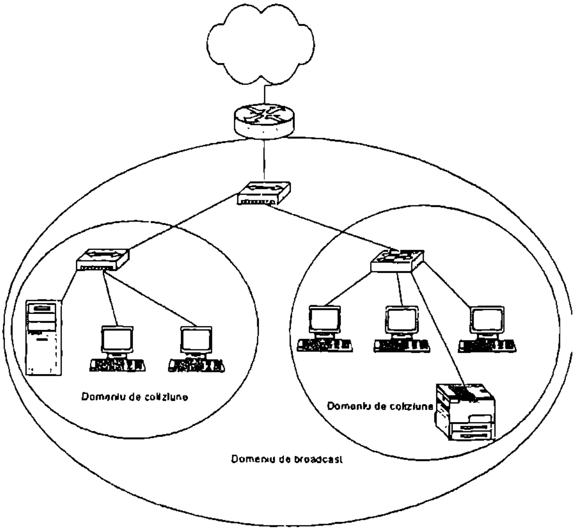


Figura 3.4.1. Domenii de coliziune și domenii de broadcast

Porţiunea de reţea în care pachetele transmise intră în coliziune se numeşte *domeniu de coliziune*. Acest fenomen apare în toate cazurile în care mediul de transmisie este partajat între mai multe calculatoare. Toate conexiunile care se fac prin intermediul dispozitivelor de nivel 1 fac parte dintr-un domeniu de coliziune.

Pachetele implicate într-o coliziune sînt distruse bit cu bit. Spuneam că pentru a se evita astfel de situaţii, reţeaua trebuie să deţină un mecanism (CSMA/CD, de exemplu) prin care să gestioneze conflictele care apar. În funcţie de tehnologia folosită, numărul calculatoarelor care pot folosi împreună un mediu de transmisie (denumit *segment*) este limitat.

Despre hub-uri (repetoare) am spus că sînt dispozitivele care regenerează traficul unei reţele fără însă a filtra în vreun fel informaţiile pe care le recepţionează/transmit. Informaţiile primite de un port al unui hub sînt transmise tuturor celorlalte porturi. Prin urmare, folosirea acestor dispozitive conduce la extinderea unui domeniu de coliziune.

Există o regulă care trebuie respectată în reţelele Ethernet: *numărul maxim de hub-uri între două calculatoare din reţea trebuie să fie 4*! Aceasta deoarece fiecare hub induce latenţă, iar depăşirea acestui număr duce la creşterea numărului de coliziuni întîrziate. Coliziunea întîrziată apare după transmiterea primilor 64 bytes din cadru. Chipseturile plăcilor de reţea nu au capacitatea de a retransmite informaţiile în urma apariţiei unei coliziuni întîrziate.

În practică această regulă este cunoscută sub denumirea 5-4-3-2-1 : cinci secţiuni de reţea, 4 repetoare, 3 segmente cu host-uri, 2 segmente de legătură şi un domeniu de coliziune.

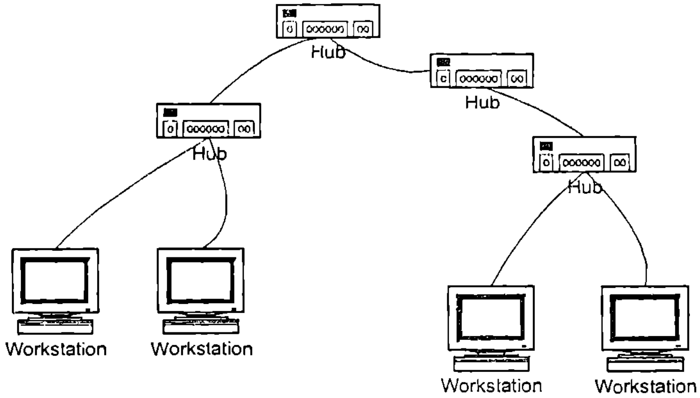


Figura 3.4.2. Regula 5-4-3-2-1

Chiar dacă sînt dispozitive ieftine, repetoarele sînt principalele echipamente care contribuie la extinderea domeniilor de coliziune. Rezolvarea acestui neajuns constă în *segmentarea reţelei* cu ajutorul switch-urilor şi routerelor.

Două sînt motivele pentru care vom dori să segmentăm o reţea:

- izolarea traficului între segmentele reţelei;
- obţinerea unei lăţimi de bandă mai mari pentru utilizatori, prin crearea unor domenii de coliziune reduse.

Fără segmentare, o rețea mai mare decît cea destinată unui grup de lucru (de obicei, maximum 10 calculatoare) va deveni foarte repede „inundată” de coliziuni, ba chiar virtual ar ajunge în situația de a nu mai avea disponibilă lățime de bandă.

O rețea Ethernet care folosește switch-uri conduce la o topologie care se comportă ca și cînd ar exista doar două noduri în respectiva rețea : un nod sursă și un nod destinație. Aceste două noduri partajează, de exemplu, 10 Mbps între ele, ceea ce înseamnă întreaga lățime de bandă disponibilă pentru transmisia datelor. Folosirea acestor echipamente permite rețelei să funcționeze mult mai eficient, deoarece disponibilitatea lățimii de bandă se apropie de 100%.

În cazul unui switch, fiecare nod reprezintă o conexiune către un segment de rețea. Crearea acestor microsegmente de rețea conduce la eliminarea coliziunilor dintr-un domeniu. Fiecare nod este conectat direct la un port al switch-ului sau la un segment care este conectat la un port. Prin aceasta se creează o conexiune pe 10 Mbps între fiecare nod și pentru fiecare segment al switch-ului. Un calculator conectat direct la un port al switch-ului va reprezenta propriul său domeniu de coliziune și va avea acces la întreaga lățime de bandă : 10Mbps.

Switch-ul citește adresa sursă și/sau destinație a fiecărui cadru pe care îl primește. În funcție de informațiile acumulate va hotărî ce decizie trebuie luată : dacă trebuie comutat către un alt segment sau nu.

Dacă switch-ul este considerat un echipament pasiv ce acționează doar la nivelul legătură date, routerul acționează la nivelul rețea și ia decizii pe baza adreselor folosite de protocoalele acestui nivel. Acest lucru presupune examinarea adreselor destinație conținute în fiecare pachet și consultarea tabelelor de rutare cu privire la instrucțiunile ce trebuie urmate.

Cu ajutorul acestor echipamente se atinge cel mai ridicat nivel de segmentare datorită capacității lor de a decide cu exactitate unde trebuie să ajungă un pachet și ce cale trebuie să urmeze. Aceste acțiuni induc însă, inevitabil, latență.

CAPITOLUL 4

Nivelul rețea

Nivelul rețea joacă un rol important în transmisia datelor: folosește o schemă de adresare pe care se bazează echipamentele pentru a determina care este destinația datelor transmise.

Protocoalele care nu sînt suportate de nivelul 3 pot fi folosite doar în rețelele de dimensiuni mici. Aceste protocoale folosesc, de obicei, un nume pentru a identifica un calculator din rețea (cum ar fi adresa MAC). Dar, pe măsură ce rețeaua se dezvoltă, organizarea acestor nume devine un calvar. Dacă vrem să interconectăm între ele două subrețele, va trebui să verificăm dacă numele calculatoarelor din cele două subrețele nu sînt duplicate.

Internetul a ajuns astăzi o colecție de segmente de rețea care partajează în comun resurse informaționale. Echipamentele de nivel 3 folosite la interconectarea rețelelor sînt routerele. Acestea sînt capabile să ia decizii logice cu privire la traseul cel mai bun pe care trebuie să-l urmeze un pachet prin rețea.

4.1. Identificarea traseului

Traseul (ruta) pe care îl are de parcurs un pachet este determinat în cadrul nivelului rețea. Funcția prin care este identificat traseul permite routerului să evalueze posibilele trasee pe care le are la dispoziție un pachet pentru a ajunge la destinație. Serviciile pentru rutare folosesc informațiile despre topologia rețelei pentru a evalua aceste rute. Determinarea traseului (se mai numește și rutare) reprezintă procesul la care face apel un router pentru a alege cea mai bună cale pe care trebuie să o urmeze un pachet pentru a ajunge la destinație.

Acest proces poate fi comparat cu conducerea unei mașini de la Iași la Neptun, de exemplu. Avem nevoie de o hartă pentru a stabili care este traseul optim (din punct de vedere al timpului și combustibilului consumat) pe care trebuie să-l parcurgem pentru a ajunge la Neptun.

Adresele de rețea identifică parțial drumul folosit de un router pentru transmisia unui pachet într-o rețea: care este sursa și destinația unui pachet. Gîndiți-vă la sistemul de telefonie: fiecare oraș, țară, continent au un cod unic de identificare. Fiecare abonat are un număr de telefon!

Dacă la nivelul 3 nu ar exista o schemă de adresare similară cu exemplul anterior, rutarea nu ar putea avea loc. Routerul are nevoie de adrese de rețea (atribuite în mod

ierarhic) pentru a putea transfera în mod corespunzător pachetele către destinaţie (vezi şi *http : //www.rad.com/networks/1997/nettut/router.html*).

Majoritatea dispozitivelor de reţea deţin atît o adresă MAC, cît şi o adresă specifică unui anumit protocol. Cînd un calculator este mutat dintr-o reţea în alta, îşi păstrează adresa MAC, dar îşi modifică adresa de reţea. Adresa MAC o putem compara cu numele noastre : o dată declarat, numele unei persoane poate fi mai greu schimbat. Adresa de reţea o putem compara cu adresa domiciliului : astăzi sînteţi flotanţi. Mîine...

Principala funcţie a nivelului reţea o reprezintă găsirea celui mai bun drum pe care trebuie să-l parcurgă un pachet prin reţea, de la sursă la destinaţie. Aminteam, la un moment dat, că sînt două metode de adresare : ierarhizată şi non-ierarhizată.

Schema de adresare non-ierarhizată atribuie unui echipament următoarea adresă disponibilă dintr-o listă dată. Această schemă se aseamănă cu mecanismul după care se alocă mărcile angajaţilor într-o firmă.

Adresele MAC funcţionează în această manieră. Un producător de plăci de reţea primeşte o secvenţă de numere ce pot fi atribuite respectivelor dispozitive.

Spre deosebire de aceasta, adresarea ierarhizată nu foloseşte alocarea aleatorie a unei adrese, ci mai degrabă în funcţie de localizarea unei staţii de lucru. O astfel de schemă de adresare este adresarea IP, care are o structură specifică şi care nu alocă aleator adresele.

Internet Protocol reprezintă cea mai folosită schemă de adresare ierarhică la nivelul 3. Dacă aruncăm o privire asupra modelului OSI, vom observa că pe măsură ce informaţiile străbat în jos nivelurile acestui model, datele sînt încapsulate la fiecare nivel. La nivelul reţea datele sînt transformate în datagrame, şi dacă reţeaua foloseşte adresarea IP, datele sînt transformate în datagrame IP.

4.2. Protocolul IP[1]

```
Captured at   +00 00.592
Length: 140    From: User    Status: Ok
IP: Version = 4                             <46>
IP: IHL = 24 [Bytes]                        <46>
IP: Type of Service. 0x00                   <00>
IP:    Routine
IP:    Normal Delay
IP:    Normal Throughput
IP:    Normal Reliability
IP: Total Length = 284                      <011C>
IP: Identifiers = 13973                     <3695>
IP: Flags: 0x00                             <00>
IP:    May Fragment
IP:    Last Fragment
IP: Fragment Offset = 0 [Bytes]             <0000>
IP: Time to Live = 15 [Seconds/Hops]  <0F>
IP: Protocol: 1 ICMP                        <01>
IP: Header Checksum = 0x2CC9                <2CC9>
IP: Source Address = 180.180.2.4            <B4B40204>
IP: Destination Address = 200.200.200.2  <C8C8C802>
IP: Option = 1 [No Operation]               <01>
IP:    Copy Flag = 0
IP:    Option Class = 0 [Datagram or network control]
IP:    Option Number = 1
IP: Option = 1 [No Operation]               <01>
IP:    Copy Flag = 0
IP:    Option Class = 0 [Datagram or network control]
```

Elementul central al Internetului este protocolul de nivel reţea numit **IP (Internet Protocol)**. Sarcina acestui protocol este de a oferi o cale pentru a transporta datagramele de la sursă la destinaţie, fără a ţine seama dacă maşinile sînt sau nu în aceeaşi reţea, sau dacă sînt sau nu alte reţele între ele. Teoria spune că datagramele IP pot să aibă fiecare pînă la 64K octeţi, dar în practică acestea au în jur de 1500 octeţi. Fiecare dintre aceste datagrame este transmisă prin Internet, eventual fragmentată în unităţi mai mici. Cînd toate aceste unităţi ajung la destinaţie, ele sînt reasamblate

1. Aşa cum este descris prin IETF RFC791.

de nivelul reţea formînd datagrama originală, care este pasată nivelului transport de pe maşina receptoare.

O datagramă IP este alcătuită dintr-o parte de *antet* (*header*) şi o parte de *text*. Antetul are o parte fixă de 20 octeţi şi o parte opţională cu lungime variabilă. Structura antetului IP este prezentată în continuare:

<table>
<tr><th>4 biţi</th><th>4 biţi</th><th>8 biţi</th><th colspan="2">16 biţi</th></tr>
<tr><td>Versiune</td><td>IHL</td><td>Tip serviciu</td><td colspan="2">Lungime totală</td></tr>
<tr><td colspan="3">Identificare</td><td>Flags (3biţi)</td><td>Deplasament fragment
(Fragment offset)</td></tr>
<tr><td colspan="2">Timp de viaţă (TTL)</td><td>Protocol</td><td colspan="2">Sumă de control</td></tr>
<tr><td colspan="5">Adresă sursă</td></tr>
<tr><td colspan="5">Adresă destinaţie</td></tr>
<tr><td colspan="5">Opţiuni</td></tr>
</table>

Cîmpul *Versiune* memorează versiunea protocolului căruia îi aparţine datagrama transmisă. Astfel devine posibilă tranziţia dintre versiunile aceluiaşi protocol (de la IPv4 la IPv6, de exemplu).

Cîmpul *IHL* (*Internet Header Length*) specifică cît de lung este antetul (spuneam că lungimea sa nu este constantă) în cuvinte de 32 biţi. Valoarea minimă este 5 şi se aplică atunci cînd nu sînt prezente alte opţiuni.

Tip serviciu este cîmpul care permite sursei să comunice ce tip de serviciu doreşte: fiabil, rapid sau o combinaţie. La rîndul său, acest cîmp conţine un subcîmp numit *precedenţă* şi 3 flaguri (indicatori): D, T, R. Subcîmpul *precedenţă* are o lungime de 3 biţi şi stabileşte priorităţile de la 0 la 7:

Valoare	Descriere
0	Normal.
1	Prioritate.
2	Imediat.
3	Flash.
4	Flash override.
5	CRITIC/ECP.
6	Internetwork control.
7	Network control.

Cei trei indicatori (flaguri) permit sursei să stabilească care factori o afectează cel mai mult: întîrzierea, *throughput*-ul[1] (productivitatea) sau fiabilitatea. Aceste cîmpuri au fost introduse pentru a sprijini deciziile pe care le au de luat routerele. Majoritatea routerelor ignoră însă aceşti indicatori.

1. Cantitatea de date pe care un protocol de la nivelul transport o poate transfera pe unitatea de timp.

Valoare D	Descriere
0	Întîrziere normală.
1	Întîrziere redusă.

Valoare T	Descriere
0	Productivitate normală.
1	Productivitate ridicată.

Valoare R	Descriere
0	Fiabilitate normală.
1	Fiabilitate ridicată.

Cîmpul *lungime totală* se referă la întregul conţinut al datagramei : antetul şi datele. Lungimea maximă este de 65535 octeţi. La ora actuală pot fi transmise datagrame mai mari de această dimensiune doar în măsura în care destinatarul este capabil să le accepte.

Prin intermediul cîmpului *identificare* destinatarul unei datagrame determină cărei datagrame aparţine un anumit pachet. Toate fragmentele unei datagrame conţin aceeaşi valoare de identificare.

Cîmpul *deplasamentul fragmentului* este precedat de două *indicatoare : DF* şi *MF.* DF (*Don't Fragment*) indică routerelor să nu fragmenteze o datagramă deoarece calculatorul destinaţie nu este capabil să o asambleze la loc. Toate calculatoarele trebuie să accepte fragmente de 576 octeţi sau mai mici.

Valoare DF	Descriere
0	Fragmentează dacă este necesar.
1	Nu fragmenta.

MF (*More Fragments*) este indicatorul care arată dacă toate fragmentele unei datagrame au ajuns la destinaţie. Toate fragmentele, cu excepţia ultimului, au acest indicator activat.

Valoare MF	Descriere
0	Acesta este ultimul fragment.
1	Urmează alte fragmente.

După aceşti indicatori spuneam că urmează *deplasamentul fragmentului* care indică locul fragmentului curent în cadrul datagramei. Toate fragmentele unei datagrame, cu excepţia ultimului, trebuie să fie multipli de 8 octeţi. Cum acest cîmp are o lungime de 13 biţi, înseamnă că există maximum 2^{13} fragmente pe datagramă (8192) şi o lungime maximă a acesteia de 65536 octeţi!

Timpul de viaţă este un contor folosit pentru a limita durata de viaţă a pachetelor. Acest timp este măsurat în secunde, avînd o valoare maximă de 255 secunde. Prin intermediul său se previne ca un pachet să circule la infinit prin reţea. În practică, TTL contorizează doar hop-urile (salturile, routerele) dintr-o reţea în alta.

După ce reasamblează datagramele, nivelul reţea trebuie să ştie ce să facă mai departe cu aceasta. În acest moment intervine cîmpul *protocol* care spune nivelului reţea cărui

proces de transport trebuie pasată datagrama (în continuare sînt prezentate cele mai cunoscute protocoale[1]).

Valoare	Protocol
1	ICMP - Internet Control Message Protocol.
2	IGMP - Internet Group Management Protocol. RGMP - Router-port Group Management Protocol.
6	TCP - Transmission Control Protocol.
8	EGP - Exterior Gateway Protocol.
9	IGRP - Interior Gateway Routing Protocol.
17	UDP - User Datagram Protocol.
41	IPv6 over IPv4.
88	EIGRP.
89	OSPF - Open Shortest Path First Routing Protocol. MOSPF - Multicast Open Shortest Path First.
255	Reserved.

Suma de control a antetului trebuie recalculată de fiecare dată cînd antetul unei datagrame se modifică (de obicei, la trecerea dintr-o rețea în alta) și detectează erorile generate de memoria routerelor.

Despre cîmpurile *adresă sursă* și *adresă destinație* discutăm în paragrafele următoare. Ele indică cine este la originea datagramei și cine este destinatarul acesteia.

Cîmpul *opțiuni*, a cărui lungime este variabilă, a fost inclus pentru a permite dezvoltarea versiunilor viitoare ale protocolului.

Cele mai importante opțiuni sînt :

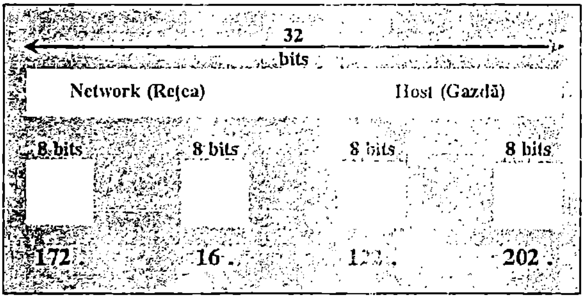
Opțiune	Valoare	Lungime	Descriere
2 - Securitate	130	11	Cît de secretă este datagrama
3 - Dirijare aproximativă pe baza sursei	131	Variabilă	Lista routerelor care nu trebuie sărite
4 - Amprenta de timp	68	Variabilă	Fiecare router își adaugă adresa și o adresă de timp
7 - Înregistrează calea	7	Variabilă	Fiecare router își adaugă adresa
9 - Dirijare strictă pe baza sursei	137	Variabilă	Indică calea completă de parcurs

4.3. Adresarea IP

Dacă ați înțeles cele spuse pînă acum, nu ar trebui să aveți prea multe probleme în continuare. Dacă nu, s-ar putea ca rîndurile care urmează să vă inducă un ușor disconfort.

O adresă IP conține informațiile necesare pentru a transporta un pachet cu date prin rețea și este reprezentată printr-un număr binar cu o valoare egală cu 32 biți.

1. Numerotarea protocoalelor este definită prin RFC1700.



Pentru a putea fi uşor de citit, adresa IP a fost împărţită în patru octeţi, fiecare octet conţinînd 8 biţi. Valoarea maximă a fiecărui octet (în zecimal) este 255.

Orice adresă IP este logic împărţită în două zone. Prima zonă se numeşte *network id* şi identifică reţeaua căreia îi aparţine un echipament. Cea de a doua zonă se numeşte *host id* şi identifică, în mod unic, dispozitivul conectat la reţea. Deoarece o adresă IP este alcătuită din patru octeţi separaţi prin punct, primul, al doilea sau al treilea dintre aceştia pot fi folosiţi pentru a identifica reţeaua din care face parte un dispozitiv. La fel şi pentru identificarea dispozitivului în sine.

Există trei clase de adrese IP comerciale, clase gestionate de InterNIC[1] : clasa A, B sau C (mai există D şi E, dar acestea nu sînt comerciale). Clasa A este rezervată de InterNIC organizaţiilor guvernamentale (mai mult guvernelor) din lumea întreagă ; clasa B este rezervată organizaţiilor medii-mari, iar clasa C este rezervată oricărui alt tip de organizaţie.

Cînd o adresă din clasa A este scrisă în format binar, primul bit este întotdeauna *0*. Primii doi biţi ai unei adrese din clasa B sînt *10*, iar primii trei biţi ai unei adrese din clasa C sînt întotdeauna *110*. Un exemplu de adresă IP din clasa A: 124.95.44.15. Primul octet (124) identifică numărul reţelei, atribuit de InterNIC. Administratorul acestei reţele va atribui valori pentru restul de 24 biţi. O manieră uşoară, prin care puteţi să recunoaşteţi dacă un dispozitiv face parte dintr-o reţea de clasă A, presupune să analizaţi primul octet al adresei IP. Numerele din primul octet al adreselor din clasa A sînt cuprinse între 0 şi 127.

A	N	H	H	H
B	N	N	H	H
C	N	N	N	H

Toate adresele IP din clasa A folosesc doar primii 8 biţi pentru a identifica porţiunea „network" din cadrul unei adrese. Restul de trei octeţi din cadrul adresei sînt rezervaţi porţiunii „host". Cea mai mică adresă ce poate fi atribuită unui host va avea toţi biţii din cadrul ultimilor trei octeţi la valoarea 0. Cel mai mare număr ce poate fi atribuit porţiunii host va avea toţi biţii din ultimii trei octeţi la valoarea 1.

Orice reţea care face parte dintr-o clasă A de adrese IP poate să conţină teoretic 2^{24} host-uri (adică 16.777.214).

Un exemplu de adresă din clasa B : 151.10.13.28. Primii doi octeţi identifică numărul reţelei atribuit de InterNIC. Administratorul unei astfel de reţele poate să atribuie valori următorilor 16 biţi. Cînd vreţi să recunoaşteţi dacă o adresă este din clasa B, analizaţi primii doi octeţi ai adresei. Aceste adrese au întotdeauna valori cuprinse între 128-191 pentru primul octet şi între 0-255 pentru cel de al doilea octet.

Toate adresele din clasa B folosesc primii 16 biţi pentru a identifica porţiunea „network" din cadrul unei adrese. Ultimii 2 octeţi sînt rezervaţi porţiunii „host". Orice

1. Vezi www.Internic.net.

rețea care folosește adrese din clasa B poate atribui teoretic 2^{16} (65.534) adrese IP echipamentelor care sînt atașate acesteia.

O adresă din clasa C: 201.110.213.28. Primii trei octeți identifică numărul rețelei atribuit de către InterNIC. Administratorul de rețea poate atribui valori doar ultimului octet. Cum puteți recunoaște o adresă din clasa C? Analizați primii trei octeți: primul octet ia valori între 192-223, al doilea și al treilea octet pot să ia valori între 1-255. Toate adresele din clasa C folosesc primii 24 biți pentru a identifica rețeaua din care face parte un dispozitiv. Doar ultimul octet este rezervat porțiunii „host". Orice rețea care folosește adrese din clasa C poate aloca teoretic 2^8 (256) adrese echipamentelor atașate acesteia.

Orice adresă IP identifică un echipament într-o rețea și rețeaua căruia aparține. Dacă, spre exemplu, calculatorul vostru vrea să comunice cu altul din rețea, ar trebui să știți adresa IP al celui din urmă. De fapt, ar trebui să știți adresele tuturor calculatoarelor cu care vreți să comunicați. Ar fi complicat, nu? Din fericire acest neajuns este rezolvat de alții.

Adresele IP care au toată porțiunea „host" cu valoarea 0 sînt rezervate ca *adrese de rețea*. De exemplu, o adresă din clasa A 113.0.0.0 reprezintă adresa IP pentru rețeaua 113. Un router va folosi această adresă pentru a transmite datele în Internet.

Să luăm ca exemplu o adresă din clasa B. Primii doi octeți nu pot fi zero pentru că valorile lor sînt atribuite de InterNIC și reprezintă numerele rețelelor respective. Doar ultimii doi octeți pot fi 0, deoarece numerele din acești octeți reprezintă numărul host-urilor și sînt rezervate dispozitivelor atașate respectivei rețele. Pentru a putea comunica cu toate dispozitivele din rețea, adresa IP trebuie să conțină 0 în ultimii doi octeți. O astfel de adresă ar fi, de exemplu, 176.10.0.0.

Cînd se transmit date către toate echipamentele dintr-o rețea, trebuie creată o adresă de broadcast (difuzare). Broadcast-ul apare cînd stația sursă transmite date către toate celelalte dispozitive din rețea. Dar pentru a fi sigură că toate aceste dispozitive sînt „atente" la mesajul broadcast, stația sursă trebuie să folosească o adresă IP pe care să o recunoască toate celelalte echipamente din rețea. De obicei, într-o astfel de adresă, biții din porțiunea host au toți *valoarea 1*. Pentru rețeaua folosită în exemplul anterior, adresa de broadcast va fi 176.10.255.255 (vezi și *http://www.ralphb.net/IPSubnet*).

Într-o rețea, host-urile pot comunica între ele doar dacă au același identificator de rețea (porțiunea *network id* este identică). Acestea pot să partajeze același segment fizic de rețea, dar, dacă au identificatori de rețea diferiți, nu pot comunica decît dacă există un alt dispozitiv care să realizeze conexiunea între segmentele logice ale rețelei (sau identificatorii acestora). (Puteți asemui acești identificatori de rețea cu codul poștal.)

După cum am arătat deja, fiecare clasă de adrese IP permite un număr fix de host-uri. Dar nu trebuie să uitați că *prima* adresă din fiecare rețea este rezervată pentru a *identifica rețeaua*, iar ultima *adresă* este rezervată pentru *broadcast*.

Clasa	Valoarea zecimală a primului octet	Rețele	Numărul total de rețele valide	Numărul de host--uri/rețea	Numărul de bytes din porțiunea network	Numărul de bytes din porțiunea host
A	1-126	1.0.0.0 126.0.0.0	2^7-2	2^{24}-2	1	3
B	128-191	128.1.0.0 191.254.0.0	2^{14}-2	2^{16}-2	2	2
C	192-223	190.0.1.0 223.255.254.0	2^{21}-2	2^8-2	3	1

4.4. Adresarea IP în subrețele

De cele mai multe ori, în practică, pentru o mai mare flexibilitate, administratorii de rețea sînt nevoiți să împartă o rețea în mai multe subrețele. Similar cu porțiunea „host" din cele trei clase de adrese, adresele pentru subrețele pot fi atribuite de către administratorul de rețea. Mai mult, ca și în cazul general, adresele subrețelelor sînt unice.

REȚEA	SUBREȚEA	GAZDĂ

Adresa pentru o subrețea include: numărul (identificatorul) rețelei, numărul subrețelei și numărul host-ului. Pentru a crea o subrețea, administratorul trebuie să „împrumute" biți din porțiunea de host a unei clase și să-i folosească în cadrul cîmpului „subrețea". Numărul minim de biți ce pot fi împrumutați din zona host este 2! Dacă se dorește a se împrumuta doar un bit pentru a crea o subrețea, atunci vom fi în situația de a avea un singur număr pentru rețea (0) și o adresă de broadcast (1). Numărul maxim de biți ce pot fi împrumutați din porțiunea host poate fi oricare, cu condiția de a păstra cel puțin 2 biți pentru identificatorul de host.

Termenul tradițional „prefix" pentru rețele extinse sau *subnet mask*, sau *mask* se referă la identificatorul care spune dispozitivelor dintr-o rețea care parte dintr-o adresă IP reprezintă prefixul rețelei, care parte reprezintă numărul subrețelei și care este numărul host-ului. O mască de subrețea este o adresă IP și are tot 32 de biți. Biții din porțiunea *network id* și subnet au valoarea 1, în timp ce biții din porțiunea host au valoarea 0.

Într-o rețea IP, cea mai mică adresă este adresa de rețea sau identificatorul acesteia. Această afirmație este valabilă și în cazul subrețelelor: adresa cea mai mică este adresa subrețelei. Routerul este dispozitivul de rețea care realizează operații booleane (pentru a ști pe ce traseu trebuie să trimită informațiile), iar dintre acestea cea mai importantă este AND. Pentru a identifica o subrețea, routerul „înmulțește" logic adresa IP și subnet mask-ul, rezultatul obținut reprezentînd numărul rețelei/subrețelei.

Spuneam despre masca unei subrețele că este tot o adresă IP: are 32 de biți împărțiți în patru octeți. Într-o mască de rețea, toți biții din porțiunea network/subnetwork au valoarea 1, iar cei din porțiunea host, 0.

Dacă nu s-au „împrumutat" biți pentru calcularea subrețelelor, masca de rețea pentru o rețea de clasă B va fi implicit 255.255.0.0. Dacă s-ar împrumuta 8 biți din porțiunea host, masca de subrețea a acestei clase ar deveni 255.255.255.0. Deoarece porțiunea host are doar doi octeți, numărul maxim al biților ce pot fi împrumutați pentru obținerea de subrețele este 14!

Să aruncăm o privire și asupra clasei C. Porțiunea host a adreselor din această clasă are un singur octet. Prin urmare, maximumul de biți ce pot fi împrumutați pentru a crea subrețele este 6, iar minimumul este 2. Subrețelele care conțin adresa de rețea și adresa de broadcast nu pot fi folosite. Altfel spus, dacă împrumutați un singur bit, se vor crea două subrețele, dar nici una dintre acestea nu va putea fi folosită.

Valoarea oricărui octet este dată de numărul biților folosiți. Valoarea zecimală maximă a fiecărui octet este 255, iar cel mai mare număr pe 8 biți, în binar, este 11111111.

Dacă citim valorile zecimale ale acestor biți, de la stînga la dreapta vom obține: 128+64+32+16+8+4+2+1=255 ($2^7+2^6+2^5+2^4+2^3+2^2+2^1+2^0$)!

Primul lucru pe care trebuie să-l faceți atunci cînd doriți să creați subrețele: extindenți parțial porțiunea rețea din cadrul adresei peste porțiunea host.

Să luăm ca exemplu adresa de clasă B 130.5.0.0, cu subnet mask-ul 255.255.255.0. Aceasta înseamnă că au fost împrumutați 8 biți pentru subrețea, iar porțiunea rețea a adresei a fost extinsă cu 8 biți.

Să luăm ca exemplu și o adresă de clasă C (sînt cele mai folosite pe la noi): 197.15.22.31 cu subnet mask-ul 255.255.255.224. Cum ultimul octet din subnet mask are valoarea 224 (11100000 în binar), înseamnă că porțiunea network a adresei a fost extinsă cu 3 biți, ajungîndu-se la un total de 27 (24+3).

De fiecare dată cînd împrumutăm biți din porțiunea host a unei adrese este important să notăm numărul subrețelelor create. Am stabilit deja că nu putem împrumuta un singur bit pentru că nu ne folosește la nimic. Împrumutînd 4 biți vom crea 4 subrețele. De fiecare dată cînd vom mai împrumuta un bit din porțiunea host, numărul rețelelor create va crește cu o putere a lui 2. Dacă împrumutăm 3 biți, vom obține 8 subrețele sau, altfel spus, 2^3. Dacă împrumutăm 4 biți, vom obține 16 subrețele sau 2^4.

Este bine să țineți minte: *de fiecare dată cînd împrumutați cîte un bit din porțiunea host, numărul subrețelelor create crește cu 2 la puterea numărului biților împrumutați.*

Efectul imediat al unui astfel de calcul? *De fiecare dată cînd împrumutați un bit din porțiunea host a unei adrese, numărul adreselor disponibile pentru o subrețea se reduce cu o putere a lui 2.*

Să continuăm exemplul cu o adresă din clasa C. Dacă nu folosim nici o mască de rețea, înseamnă că toți biții ultimului octet sînt folosiți pentru porțiunea host. Putem astfel atribui, teoretic, 256 (2^8) adrese pentru host-uri. Să presupunem că vrem să împărțim o astfel de clasă de adrese în subrețele și împrumutăm un bit din porțiunea host. Aceasta înseamnă că numărul biților ce pot fi alocați pentru host-uri se reduce la 7, iar numărul maxim al adreselor ce pot fi obținute se reduce la 128 (2^7).

Dacă împrumutăm 2 biți din porțiunea host, numărul biților ce pot fi atribuiți pentru adresele host-urilor se reduce la 6. Numărul maxim al host-urilor ce pot fi obținute pentru fiecare subrețea în parte se reduce la 64 (2^6).

Numărul adreselor ce pot fi atribuite host-urilor dintr-o subrețea este în strînsă legătură cu numărul subrețelelor create. Pentru adresele din clasa C, cu masca de rețea 255.255.255.224, înseamnă că s-au împrumutat 3 biți din porțiunea host. S-au obținut astfel 8 subrețele, fiecare cu cîte 32 host-uri (dintre care doar 30 utilizabile!!!).

Dacă tot am deslușit subrețelele, să vedem cum se calculează numărul de rețea pentru o subrețea creată (operația se numește ANDing).

Vom lua ca exemplu o rețea din clasa B[1] (într-o firmă din Iași): 172.16.0.0, în care vrem să împrumutăm 8 biți pentru a crea subrețele. În acest caz, masca de subrețea va fi 255.255.255.0. De la București, cineva dorește să transmită un mesaj către calculatorul cu adresa 172.16.2.120.

Pentru a decide unde trebuie să transmită datele, routerul „înmulțește" (AND) această adresă (transformată în binar) cu subnet mask-ul (tot binar). Cînd aceste două numere sînt înmulțite, porțiunea host a adresei se pierde pentru că devine zero. Ceea ce rămîne

1. Chiar dacă aceste adrese nu sînt rutabile, vă rugăm să acceptați exemplul.

în urma acestei operaţiuni reprezintă numărul reţelei, inclusiv numărul subreţelei. Prin urmare, datele vor fi transmise subreţelei 172.16.2.0, iar ultimul router din cadrul reţelei va şti că pachetul trebuie transmis host-ului 120 din cadrul acestei subreţele.

	Reţea	Subreţea	Gazdă
Adresă IP gazdă 172.16.2.120	10101100 00010000	00000010	01111000
Subnet mask 255.255.255.0	11111111 11111111	11111111	00000000
Subnet	10101100 00010000 172 16	00000010 2	00000000 0

Să presupunem acum că pentru aceeaşi reţea, 172.16.0.0, am hotărît să împrumutăm 7 biţi pentru a calcula subreţele. Masca de subreţea va fi în acest caz 255.255.254.0 (cît înseamnă în binar?). De la Bucureşti se transmite un mesaj către host-ul 172.16.2.160. Routerul va înmulţi adresa host-ului cu subnet mask-ul. Diferenţa obţinută reprezintă numărul reţelei şi al subreţelelor disponibile. Dacă am împrumutat 7 biţi, înseamnă că obţinem 126 de subreţele (128-2). Cîte host-uri va conţine fiecare subreţea?

Dacă lucrurile s-ar opri aici ar fi aproape bine. Din păcate, atunci cînd decideţi să creaţi subreţele, trebuie să aveţi în vedere şi maniera în care veţi optimiza aceste subreţele şi host-urile asociate lor. De ce? Am amintit deja că nu se pot folosi prima şi ultima subreţea. De asemenea, nu se pot folosi prima şi ultima adresă din cadrul fiecărei subreţele: una este adresa de broadcast a reţelei, iar cealaltă este adresa de reţea.

Prin urmare, atunci cînd se realizează subreţele, se pierd ceva adrese. Administratorul de reţea trebuie să fie atent la procentul adreselor care se pierd în urma unor astfel de calcule.

De exemplu, cînd împrumutăm 2 biţi din porţiunea host, vom obţine 4 subreţele, fiecare a cîte 64 de host-uri. Însă doar două dintre aceste reţele vor putea fi folosite, şi doar 62 de host-uri pe reţea vor fi disponibile. Ce înseamnă acest lucru? Că avem la dispoziţie 124 de adrese în loc de 256 cîte ar fi fost înainte de împărţirea reţelei în subreţele, ceea ce se traduce printr-o pierdere de 52% !

Numărul biţilor împrumutaţi	Numărul subreţelelor create	Numărul host-urilor pe subreţea	Numărul total al host-urilor	Procent utilizare
2	2	62	124	49
3	6	30	180	71
4	14	14	196	77
5	30	6	180	71
6	62	2	124	49

În fiecare clasă de adrese IP, există anumite adrese care nu sînt atribuite de InterNIC. Acestea sînt denumite adrese private sau rezervate.

Adresa 127.0.0.1 este rezervată, fiind alocată calculatorului local (*local host*). Se mai numeşte şi adresă de *loop back* (buclă). Acest număr va fi selectat pentru accesarea serverului Web instalat pe calculatorul propriu sau pentru a testa funcţionarea cartelei de reţea.

Pentru clasa A este utilizat ID 10, adică adresele de la 10.0.0.0 la 10.255.255.255. Pentru clasa B, se folosesc ID-urile de la 172.16.0.0 pînă la 172.31.0.0. Pentru clasa C sînt disponibile adresele începînd cu 192.168.0.0 pînă la 192.168.255.0 (256 de adrese).

Vom încheia discuţia legată de subreţele cu un ultim exemplu. Pentru adresa 172.31.100.100 şi subnet mask-ul 255.255.224.0 vrem să aflăm care este numărul de subreţele şi numărul de host-uri pentru fiecare subreţea.

Informaţia	Exemplu	Regula
Adresa IP	172.31.100.100	-
Subnet mask	255.255.224.0	-
Numărul de biţi din zona network	16	Sînt daţi de clasa din care face parte adresa (A, B sau C)
Numărul de biţi din zona host	13	Numărul de biţi cu valoarea 0 din subnet mask
Numărul de biţi din zona subnet	3	32 (numărul de biţi din zona network + numărul de biţi din zona host)
Numărul de subreţele	$2^3-2=6$	$2^{\text{numărul biţilor din subnet}}-2$
Numărul de host-uri pe subreţea	$2^{13}-2=8190$	$2^{\text{numărul biţilor din host}}-2$

O listă cu toate adresele virtuale corespunzătoare clasei B o găsiţi în Anexă.

4.5. Agregarea adreselor IP şi NAT

La începutul anilor '90, IETF anunţa, pe un ton sumbru, că în martie 1994 adresele IP de clasă B vor fi epuizate. În absenţa unui nou mecanism de adresare, scalabilitatea Internetului urma să fie compromisă. Singura soluţie viabilă pe termen lung o reprezenta crearea unui nou IP cu un spaţiu de adresare mult mai larg: *IPng - Internet Protocol Next Generation* sau Ipv6 (adresare pe 128 biţi). Pe termen scurt neajunsurile au fost eliminate prin adoptarea unei arhitecturi mai flexibile: CIDR[1] - *Classless Inter-Domain Routing*.

Pînă la IPng, la neajunsurile ridicate de reducerea adreselor IP şi de saturarea tabelelor de rutare au apărut şi alte soluţii: Variable Length Subnet Masking (VLSM) - numai în cazul anumitor protocoale de rutare, Address Allocation for Private Internets, Network Address Translation, CIDR.

Schema folosită de CIDR nu se deosebeşte prea mult de Ipv4, fiind de fapt o extensie a acestuia. Flexibilitatea noii scheme este dată de biţii care identifică cele trei clase principale de adrese, cu un prefix de reţea. Conceptul de clasă dispare fiind înlocuit cu cel de *prefix*.

Superneting-ul presupune, de fapt, combinarea a două sau mai multe adrese de reţea consecutive.

Să luăm ca exemplu o adresă din fosta clasă C: 192.168.8.0. Dacă la această adresă se aplică prefixul /22 înseamnă că rămîn 10 biţi ce pot fi afectaţi host-urilor. O adresă de

1. Convenţie definită în RFC 1817 (www.ietf.org/rfc/rfc1817.txt).

clasă C nu poate însă avea 1022 de host-uri. Vom putea, de exemplu, forma patru reţele de clasă C pornind de la 192.168.8.0/22. Routerul va înţelege că încă trei reţele sînt ataşate la acesta şi orice pachet către 192.168.9.0, 192.168.10.0 sau 192.168.11.0 va fi rutat cu referire la 192.168.8.0/22. CIDR nu funcţionează decît cu blocuri de adrese IP continue.

Alocarea adreselor în astfel de blocuri conduce la ceea ce se numeşte rutare ierarhică sau agregarea rutelor : o singură rută de nivel superior poate reprezenta mai multe rute de nivel inferior în tabelele de rutare. Schema după care se face rutarea este similară sistemului telefonic : centrala apelantă analizează doar prefixul apelant după care rutează apelul către respectiva centrală.

Cum se face agregarea reţelelor ?

Reţeaua	În binar
192.168.8.0	11000000.10101000.00001000.00000000
192.168.9.0	11000000.10101000.00001001.00000000
192.168.10.0	11000000.10101000.00001010.00000000
192.168.11.0	11000000.10101000.00001011.00000000
SM : 255.255.252.0	11111111.11111111.**111111**00.00000000

După cum se vede din tabelul de mai sus, cel de al şaselea bit din octetul trei al adreselor de reţea este identic. Urmînd această regulă, toate host-urile acestor reţele vor face parte dintr-o singură reţea.

Să presupunem însă că dorim să facem superneting pornind cu reţeaua 192.168.10.0/22. Înseamnă că vom avea încă trei reţele : 192.168.11.0, 192.168.12.0, 192.168.13.0. Transformînd în binar aceste adrese vom observa că cel de-al şaselea bit al celui de-al treilea octet nu este identic. Reţele 192.168.10.0 şi 192.168.11.0 vor face parte dintr-o altă superreţea.

Pentru a afla cîte reţele au fost agregate, vom scădea din valorea celui de-al treilea octet valorea subnet mask-ului : 256-252.

NAT (*Network Address Translation*) este o funcţie implementată (în principal) la nivelul sistemului de operare al routerului (IOS) prin care un calculator care nu are o adresă IP publică poate comunica totuşi cu alte calculatoare din Internet. Funcţia NAT este de a schimba adresa IP privată într-o adresă publică. Adresa IP a fiecărui pachet sursă este schimbată cind respectivul pachet părăseşte organizaţia. Adresa destinaţie va fi şi ea modificată de fiecare dată cînd un pachet ajunge la respectiva organizaţie.

Reţeaua	În binar
192.168.10.0	11000000.10101000.00001010.00000000
192.168.11.0	11000000.10101000.00001011.00000000
192.168.12.0	11000000.10101000.00001100.00000000
192.168.13.0	11000000.10101000.00001101.00000000
SM : 255.255.252.0	11111111.11111111.**111111**00.00000000

CAPITOLUL 5

Nivelul transport

Cînd am vorbit puţin la început despre acest nivel, am spus că principala sa responsabilitate se referă la asigurarea calităţii serviciilor pe care le oferă o reţea. Principala sarcină a nivelului 4 o reprezintă transportarea şi controlarea fluxului informaţional de la sursă către destinaţie. Informaţiile trebuie să ajungă în mod sigur „curate" la destinaţie.

Înainte de a merge mai departe să luăm drept exemplu o reţea Ethernet formată din două calculatoare denumite Florin şi Marius. Florin îşi cunoaşte numele, adresa IP şi adresa MAC, deoarece acestea au fost configurate mai înainte (cînd a fost instalat sistemul de operare). Înainte ca orice aplicaţie să poată funcţiona, Florin trebuie să afle adresele IP şi MAC ale lui Marius.

Pentru a intra în posesia acestor două informaţii, Florin va apela la DNS (*Domain Name System*) şi ARP (*Address Resolution Protocol*). Florin ştie adresa DNS pentru că aceasta a fost configurată o dată cu instalarea plăcii de reţea. Prin urmare, Florin va lansa o cerere DNS către DNS-ul local, întrebîndu-l pe acesta care este adresa IP a lui Marius. DNS-ul îi va răspunde că adresa solicitată este 10.1.1.2. Dar Florin mai are nevoie şi de adresa MAC folosită de 10.1.1.2. Pentru aceasta va difuza (broadcast) o cerere ARP. O astfel de cerere este transmisă către o adresă Ethernet de difuzare (broadcast), astfel încît oricine din reţea să o poată recepţiona. Deoarece adresa IP a lui Marius este 10.1.1.2, iar cererea ARP caută adresa MAC asociată acestei adrese, Marius va răspunde cu propria adresă MAC.

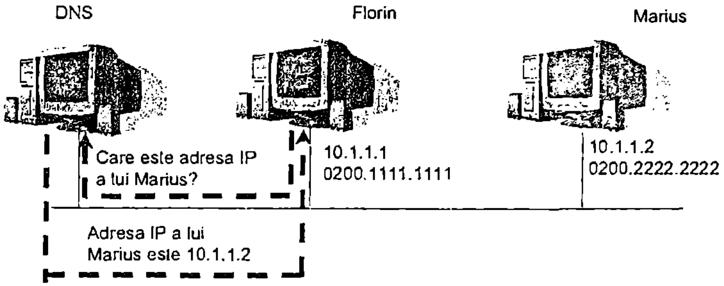


Figura 5.1. Identificarea adresei IP

Cu aceste informații obținute, Florin îi va putea trimite cadre lui Marius. Teoretic. În practică, acest lucru s-ar putea să nu funcționeze. Și dacă îl întrebați pe programator, va spune că e din cauza rețelei. Administratorul rețelei va spune că, dacă Marius răspunde la ping, problemele sînt din cauza aplicației.

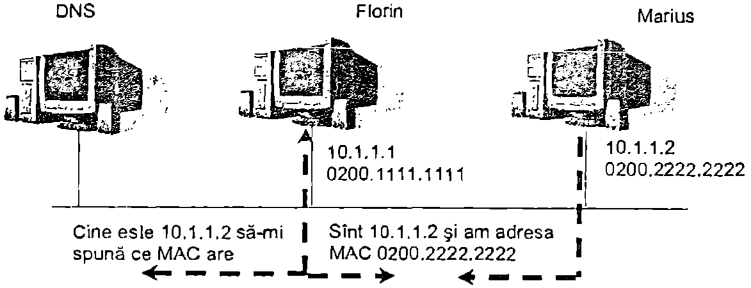


Figura 5.2. Cererea ARP

5.1. TCP Transmission Control Protocol[1]

Parte integrantă a suitei TCP/IP, TCP reprezintă protocolul orientat conexiune care oferă transmisia datelor în modul full-duplex. În figura de mai jos este prezentată structura unui fragment TCP. Înainte de a prezenta semnificația elementelor din figura următoare, facem cîteva precizări.

Prin intermediul TCP, calculatoarele schimbă informații între ele sub formă de *segmente*. Un segment este format dintr-un antet de 20 de octeți urmat de zero sau mai mulți octeți de date. Programul decide singur care este mărimea acestor segmente ținînd cont de două situații. Fiecare segment nu trebuie să depășească cei 65535 octeți de informație utilă IP. Mai mult, fiecare rețea are o unitate maximă de transfer (MTU – *maximum transfer unit*) în care trebuie să încapă segmentul TCP. Un segment care ajunge într-o rețea cu o MTU mai mică decît dimensiunea sa, va fi fragmentat de către routerul respectivei rețele.

<table>
<tr><th colspan="9">32 biți</th></tr>
<tr><th colspan="8">Port sursă (16 biți)</th><th>Port destinație (16 biți)</th></tr>
<tr><td colspan="9">Numărul secvenței</td></tr>
<tr><td colspan="9">Numărul confirmării</td></tr>
<tr><td>HLEN</td><td>Rezervat</td><td>URG</td><td>ACK</td><td>PSH</td><td>RST</td><td>SYN</td><td>FIN</td><td>Dimensiunea ferestrei</td></tr>
<tr><td colspan="8">Sumă control</td><td>Indicator urgent</td></tr>
<tr><td colspan="9">Opțiuni (cuvinte pe 32 biți)</td></tr>
<tr><td colspan="9">Date (opțional)</td></tr>
</table>

1. Descris în RFC793.

Fiecare nou segment format prin fragmentare are propriile antete TCP şi IP, această situaţie conducînd la creşterea gradului de încărcare a reţelei (fiecare segment primeşte un antet de 40 octeţi de informaţie suplimentară).

Port sursă (16 biţi) şi *port destinaţie (16 biţi)* sînt cîmpurile care identifică punctul iniţial şi pe cel final al conexiunii (în paragraful următor vom lămuri cum stă treaba cu porturile).

Cîmpul *numărul secvenţei (32 biţi)* este folosit pentru a asigura la destinaţie ordonarea corectă a informaţiilor. *Numărul confirmării (32 biţi)* se referă la următorul octet care este aşteptat la destinaţie.

HLEN - lungimea antetului TCP indică numărul de cuvinte de 32 de biţi care sînt conţinute în antetul TCP, deoarece cîmpul *opţiuni* este de lungime variabilă. Acest cîmp este urmat de 6 biţi nefolosiţi (rezervaţi pentru dezvoltările ulterioare, dar de care nu a mai fost nevoie).

Cele 6 cîmpuri de un bit au următoarea semnificaţie:

- *URG (Urgent)* - indică deplasamentul în octeţi faţă de numărul curent de secvenţă la care se află informaţia urgentă. Foloseşte îndeosebi la înlocuirea mesajelor de întrerupere.
- *ACK (Confirmare)* - indică validitatea numărului de confirmare. Dacă acest bit are valoarea zero, este ignorat cîmpul număr de confirmare al segmentului respectiv.
- *PSH (Push - Forţare)* - acest bit indică destinatarului să livreze aplicaţiei informaţia imediat ce este recepţionată, fără a o mai memora în buffer.
- *RST (Reset)* - desfiinţează o conexiune care a devenit inutilizabilă.
- *SYN (sincronizare)* - stabileşte conexiunea între calculatoare.
- *FIN (Sfîrşit)* - termină o conexiune.

TCP-ul foloseşte pentru controlul fluxului informaţional *ferestre glisante de dimensiune variabilă*. Cîmpul *dimensiunea ferestrei* indică numărul de octeţi care pot fi trimişi, începînd cu octetul confirmat.

Cîmpul *sumă de control* este calculat pentru antet şi informaţia propriu-zisă. Iniţial, acest cîmp are valoarea zero, iar cîmpul de date este completat cu un octet suplimentar nul, dacă lungimea sa este un număr impar.

Proiectat pentru a suporta facilităţi ulterioare, cîmpul *opţiune* este folosit mai ales pentru a indica lungimea maximă a unui segment TCP.

În conformitate cu RFC 793, TCP a fost proiectat să realizeze următoarele funcţii:

- multiplexare;
- refacerea în urma erorilor;
- controlul fluxului folosind ferestre;
- stabilirea şi închiderea conexiunilor;
- transferul datelor.

Multiplexarea

Este procesul prin care un calculator decide cărei aplicaţii îi sînt destinate datele recepţionate şi face apel la conceptul de *socket*. În acest context, un socket este alcătuit din trei lucruri: adresa IP, protocolul de transport folosit şi un număr de port.

Continuînd exemplul cu care am început acest capitol, să presupunem că browserul de pe calculatorul lui Florin apelează serverul Web de pe calculatorul lui Marius. În acest caz, socketul de pe calculatorul lui Marius va fi : 10.1.1.2, TCP, 80. Socketul folosit de Florin va fi : 10.1.1.1, TCP, 1030. În general, calculatoarele care lansează cereri alocă în mod dinamic porturi mai mari de 1024.

Portul este o componentă de bază a soketului folosită pentru a transmite informaţiile nivelurilor superioare şi pentru a urmări conversaţiile care au loc în acelaşi timp în reţea.

Cei care dezvoltă aplicaţii sînt nevoiţi să folosească numărul porturilor definite prin RFC 1700[1]. Conversaţiilor care nu folosesc aplicaţii cu porturi definite li se atribuie aleator numere pentru porturi. Acestea vor fi folosite ca adrese sursă şi destinaţie în cadrul segmentului TCP.

Pentru a discuta despre o conexiune TCP, trebuie stabilită mai întîi o conexiune într-un soclu de pe maşina sursă şi unul de pe maşina destinaţie. Un soclu poate fi folosit pentru mai multe conexiuni.

Numerele de port mai mici de 255 se numesc *porturi general cunoscute* şi sînt rezervate serviciilor standard. Porturile din intervalul 256-1023 sînt folosite de companiile publice care dezvoltă aplicaţii specifice, iar cele peste 1024 se atribuie aleator.

Fiecare calculator face apel la un anumit port pentru a rula o aplicaţie. Calculatorul sursă foloseşte un port atribuit dinamic în momentul în care lansează o cerere, port care de obicei are un număr mai mare decît 1023.

Lista completă cu numerele porturilor o găsiţi la adresa http://www.iana.org/assignments/port-numbers. Noi le vom aminti aici doar pe cele mai uzuale :

Numărul portului TCP	Descriere
20	FTP server (canalul pentru date)
21	FTP server (canalul de control)
23	Telnet server
53	Domain Name System
80	Web server (HTTP)
139	NetBIOS

Refacerea în urma erorilor (siguranţă)

Pentru a oferi siguranţă în timpul transportului, TCP numără bytes folosind cîmpurile *numărul secvenţei* şi *numărul de confirmare* din antetul segmentului.

În figura următoare, cîmpul *confirmare (ACK)* trimis de client către server atenţionează asupra următorului byte care trebuie recepţionat. Această situaţie se numeşte *forward acknowledgment*.

Să presupunem însă că cel de-al doilea segment transmis de server conţine erori sau s-a pierdut pe drum. În acest caz, clientul transmite un cîmp confirmare egal cu 2000, ceea ce înseamnă că aşteaptă bytes cu numărul 2000. Funcţia TCP a serverului Web poate reface datele prin retransmiterea segmentului cu numărul 2000 şi apoi aşteaptă confirmarea recepţiei celor 400 de bytes.

1. www.rfc-editor.org.

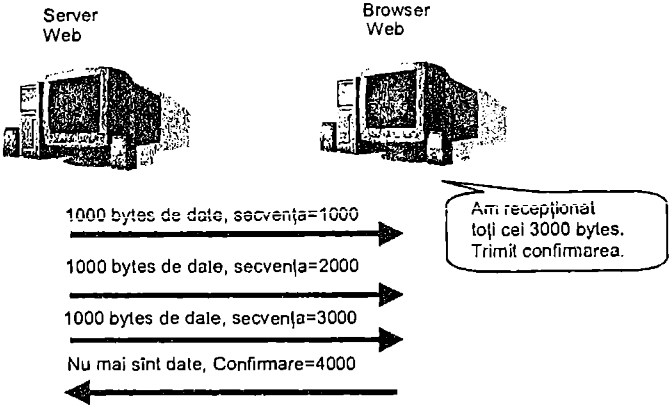


Figura 5.1.1. Numărul secvenţei şi confirmarea

Controlul fluxului folosind ferestre

Cîmpul *dimensiunea ferestrei* din cadrul segmentului TCP determină cantitatea de date care poate fi transmisă simultan, fără a fi nevoie de vreo confirmare. Despre ce este vorba ! Cînd un calculator transmite numărul de bytes care determină mărimea ferestrei, trebuie să primească o confirmare din partea destinatarului înainte de a transmite alt mesaj. De exemplu, dacă mărimea ferestrei este 1, calculatorul sursă trebuie să confirme recepţia fiecărui segment înainte ca sursa să-l transmită pe următorul. De aici rezultă o utilizare total ineficientă a lăţimii de bandă.

Three-way handshake/open connection sau *înţelegerea în trei paşi* este folosită pentru a sincroniza conexiunea între calculatorul sursă şi cel destinaţie înainte ca datele să fie transferate între acestea. Schimbul numerelor care reprezintă secvenţa este folosit pentru a se asigura că datele ce se pierd din cauza problemelor care pot apărea în reţea pot fi recuperate.

TCP foloseşte un sistem de confirmare în expectativă (tehnică care se numeşte *sliding window* – fereastră glisantă), adică numărul confirmării se referă la următorul octet care se aşteaptă a fi recepţionat. Partea glisantă din cadrul ferestrei se referă la faptul că mărimea ferestrei este negociată în mod dinamic în timpul unei sesiuni TCP.

TCP ordonează segmentele într-o anumită secvenţă prin transmiterea către destinaţie a unei informări ce poartă denumirea de confirmare. Fiecare datagramă este numerotată înainte de a fi transmisă. La destinaţie, TCP reasamblează segmentele pentru a forma mesajul iniţial. Dacă numărul unei secvenţe lipseşte din cadrul seriei pe care trebuia să o recepţioneze staţia destinaţie, segmentul va fi retransmis. Segmentele a căror recepţie nu este confirmată într-o perioadă dată de timp trebuie retransmise.

Stabilirea şi închiderea conexiunilor

Stabilirea conexiunii se referă la procesul prin care sînt iniţializate cîmpurile *numărul secvenţei* şi *confirmare* precum şi porturile care vor fi utilizate. Aici intră în acţiune, pe de o parte, cîmpul SYN (sincronizează numerele de secvenţă) care este componenta în

baza căreia se iniţializează sesiunea TCP, iar pe de altă parte, cîmpul ACK (cîmpul confirmare este valid pentru acest antet). Pînă ce nu este iniţializat numărul secvenţei, cîmpul confirmare nu joacă nici un rol.

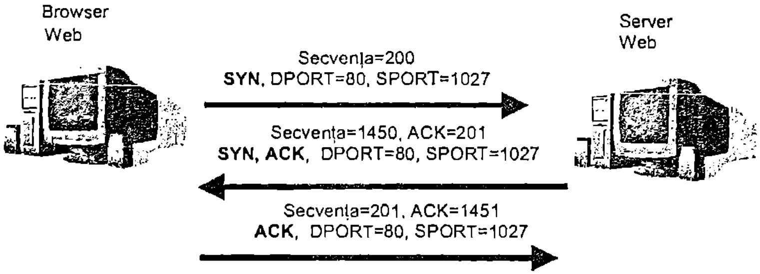


Figura 5.1.2. Stabilirea şi închiderea unei conexiuni

După cum se vede şi din fig. 5.1.2, în primul segment TCP nu este inclus nici un număr de confirmare, deoarece încă nu putem avea un astfel de număr valid sau, altfel spus, nu există nimic de confirmat.

Pentru închiderea unei sesiuni intră în acţiune cîmpul FIN prin care se atrage atenţia asupra faptului că una dintre părţi întrerupe sesiunea şi nu va fi nevoie de retransmiterea unor segmente.

Transferul datelor

Se referă nu numai la retransmiterea segmentelor care conţin erori, ci şi la ordonarea segmentelor ale căror numere de secvenţă nu sînt consecutive.

5.2. UDP - User Datagram Protocol[1]

UDP reprezintă protocolul nivelului transport care nu este orientat conexiune. Acest protocol este folosit pentru a transmite datagrame fără a fi nevoie de confirmarea recepţiei sau de garantarea transmiterii acestora. Retransmiterea datelor în caz de erori trebuie „ordonată" de alte protocoale.

32 biţi	
Port sursă (16 biţi)	Port destinaţie (16 biţi)
Lungime UDP	Sumă de control UDP

UDP este proiectat pentru aplicaţiile ce nu trebuie să recompună segmentele cu date. Altfel spus, protocoalele de la nivelul aplicaţii sînt direct răspunzătoare de siguranţa datelor transmise. Protocoalele care folosesc UDP sînt: TFTP, SNMP, DHCP, DNS.

1. Descris în RFC768.

Diferenţa principală faţă de TCP constă în faptul că nu există nici un mecanism de detectare a erorilor. Aplicaţiile care fac apel la UDP, dacă nu au propriul mecanism de recuperare a informaţiilor, sînt susceptibile să le piardă şi să fie nevoie să le transmită în totalitate. Pe de altă parte, aceste aplicaţii nu mai sînt „încetinite" de procesul de confirmare şi memoria este mult mai rapid disponibilizată pentru lucru.

Principalele porturi UDP sînt:

Numărul portului UDP	Descriere
53	DNS
69	Trivial File Transfer Protocol (TFTP)
137	NetBIOS - serviciul de nume
138	NetBIOS serviciul datagrame
161	Simple Network Management Protocol (SNMP)
520	Routing Information Protocol (RIP)

5.3. ARP - protocolul de rezoluţie a adresei[1]

Spuneam că un pachet trebuie să conţină atît adresa MAC, cît şi adresa IP a destinatarului. Dacă una dintre aceste adrese lipseşte, datele nu vor mai fi transferate de la nivelul 3 către celelalte niveluri ale modelului OSI. În acest caz, cele două adrese se verifică una pe cealaltă. După ce o staţie identifică adresa IP a destinatarului, poate să adauge pachetului şi adresa MAC.

Există o mulţime de variante prin care un calculator poate determina adresa MAC pe care trebuie să o adauge datelor în timpul încapsulării. Cele mai multe dintre acestea presupun înregistrarea tuturor adreselor MAC şi IP ale echipamentelor care sînt conectate în aceeaşi reţea. Aceste înregistrări se numesc tabele **ARP (Adress Resolution Protocol)** şi prin intermediul lor, o adresă IP este mapată pe adresa MAC corespunzătoare.

Tabelele ARP reprezintă secţiuni din memoria RAM a staţiilor de lucru. Fiecare calculator din reţea are propria tabelă ARP, şi cînd doreşte să transmită ceva, face apel la aceasta.

Cînd staţia sursă transmite către o destinaţie a cărei adresă IP este cunoscută, se va consulta tabela ARP pentru a se localiza adresa MAC a destinaţiei. Dacă IP localizează o astfel de înregistrare în tabela ARP (adresă IP destinaţie-adresă MAC destinaţie), va asocia adresa IP adresei MAC identificată şi va folosi aceste adrese pentru încapsularea datelor.

Ce se întîmplă însă cînd staţia sursă nu identifică în tabela ARP adresa MAC a staţiei destinaţie? În acest caz, staţia sursă iniţiază un proces numit cerere ARP, proces care îi permite să descopere adresa MAC a staţiei destinaţie.

Cererea ARP implică crearea unui pachet care va fi trimis tuturor staţiilor din reţea. Pentru a se asigura că toate calculatoarele vor recepţiona cererea ARP, staţia sursă foloseşte o adresă MAC de broadcast: conform schemei de adresare MAC, într-o astfel de adresă toate valorile sînt F (adresa de broadcast va avea formatul FF-FF-FF-FF-FF-FF).

---

1. Descris în RFC826.

Deoarece pachetele care conţin cererea ARP traversează reţeaua în modul broadcast, vor fi recepţionate de către toate calculatoarele. Cînd o staţie recepţionează un astfel de pachet, îl transmite spre examinare nivelului reţea. Dacă adresa IP a staţiei respective corespunde adresei IP din cererea ARP, aceasta va răspunde staţiei sursă prin transmiterea propriei adrese MAC. Această operaţie este denumită, de obicei, răspuns ARP.

În momentul în care staţia care a lansat cererea ARP primeşte răspuns, extrage adresa MAC din antet şi îşi actualizează tabela ARP. În acest moment, staţia sursă va putea încapsula datele (la nivelul 3 şi 4), folosind ambele adrese ale staţiei destinaţie.

Ce se va întîmpla însă la destinaţie? Nivelul legătură date al staţiei destinatare extrage din antet adresa MAC pe care o compară cu adresa sa. Dacă cele două adrese sînt identice, datele sînt transferate nivelului reţea. Acesta le examinează şi „vede" că adresa IP destinaţie conţinută în antetul IP corespunde cu adresa sa. Tot nivelul reţea extrage antetul IP şi transferă restul datelor încapsulate nivelului transport. Acest proces se repetă pînă în momentul în care restul pachetului, parţial decapsulat, ajunge la nivelul aplicaţie unde vor putea fi citite datele.

Am aflat deja că pentru a putea comunica, două calculatoare aflate în reţele diferite mai au nevoie pe lîngă adresa IP şi de adresa *default gateway*: adresa IP a interfeţei routerului prin care se conectează respectivul segment de reţea. Adresa IP a gateway-ului trebuie să fie în aceeaşi reţea ca şi staţia respectivă.

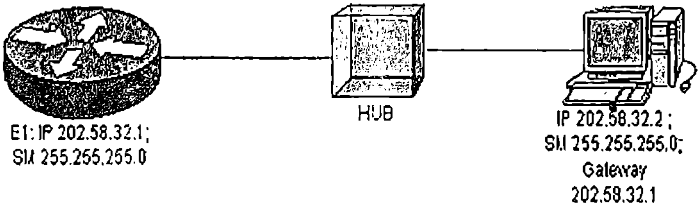


Figura 5.3.1. *Default gateway*

Dacă nu se precizează care este gateway-ul reţelei, comunicarea devine posibilă doar între calculatoarele aflate pe acelaşi segment logic de reţea. Calculatorul care doreşte să transmită date trebuie să compare adresa IP a destinatarului cu înregistrările din tabela ARP. Dacă în ARP nu se găsesc înregistrări, calculatorul sursă nu are nici o adresă IP destinaţie şi datele nu vor putea fi transmise.

Nu încercaţi să vedeţi pe bucăţi lucrurile prezentate pînă acum, pentru că ajungem la una dintre problemele cele mai importante: cum comunică două calculatoare care se află în segmente de reţea diferite (atît fizic, cît şi logic). Calculatorul sursă trebuie totuşi să ştie către cine trimite datele. Şi calculatorul destinaţie trebuie să ştie cum să interpreteze datele primite.

Am văzut deja că ARP foloseşte pachete broadcast în anumite momente. Routerul, în schimb, nu transmite mai departe pachetele broadcast (cu excepţiile de rigoare). Un calculator care doreşte să trimită date către o staţie care se află în alt segment de reţea va trimite aceste date către gateway. Prin „înmulţirea" (AND) adresei IP cu subnet mask-ul, calculatorul sursă determină adresa de reţea a segmentului respectiv. Dacă

staţia destinaţie nu este în acelaşi segment de reţea, sursa transmite datele către gateway. Dacă staţia sursă nu cunoaşte adresa MAC a gateway-ului (nu exista în tabela ARP), lansează o cerere ARP la care răspunde gateway-ul. Tabela ARP a routerului conţine înregistrările tuturor reţelelor conectate direct la acesta.

Mai există o variantă ARP denumită proxy ARP, folosită în reţele de dimensiuni mici şi lipsite de complexitate. În această variantă, o singură adresă IP este mapată pe mai multe adrese MAC. Un router pe care rulează proxy ARP, captează pachetele ARP şi răspunde cu adresa MAC corespunzătoare.

Spuneam că interfaţa sau portul prin care routerul se conectează la reţea este considerată parte a reţelei şi, prin urmare, are propria adresă IP. Routerul transmite şi recepţionează datele din reţea, construind tabele ARP prin care mapează adresele IP la adresele MAC ale participanţilor. Routerul poate fi conectat la mai multe reţele sau subreţele.

În general, echipamentele unei reţele mapează adresele IP la adresele MAC doar în cazul dispozitivelor pe care le „văd" în mod regulat. Aceasta înseamnă că un anumit echipament conţine astfel de informaţii numai cu privire la alte două dispozitive ale reţelei din care face parte. Despre ce se întîmplă în afara reţelei/subreţelei din care face parte, se cunosc foarte puţine informaţii.

Tabelele ARP realizate de un router conţin informaţii despre toate reţelele/subreţelele conectate la acesta. Pe lîngă maparea adreselor IP la adresele MAC, routerul mapează şi porturi/interfeţe.

Ce se întîmplă dacă la un router ajunge un pachet a cărui destinaţie este o reţea la care respectivul router nu este conectat? Pe lîngă adresele IP şi MAC ale echipamentelor din reţelele la care este conectat, routerul mai deţine şi adresele IP şi MAC ale altor routere. Acestea sînt folosite pentru a direcţiona datele către destinaţia finală atunci cînd adresa destinaţie a unui pachet recepţionat nu se află în tabela sa de rutare. Routerul transmite acest pachet către un alt router care pare să conţină informaţii despre destinatar în tabela sa de rutare.

Tabela ARP este folosită doar pentru a rezolva cererile din reţelele locale. Cum se desfăşoară procesul de rutare, cînd o staţie cere servicii care nu pot fi satisfăcute de routerul local, dar nici nu ştie adresa altui router?

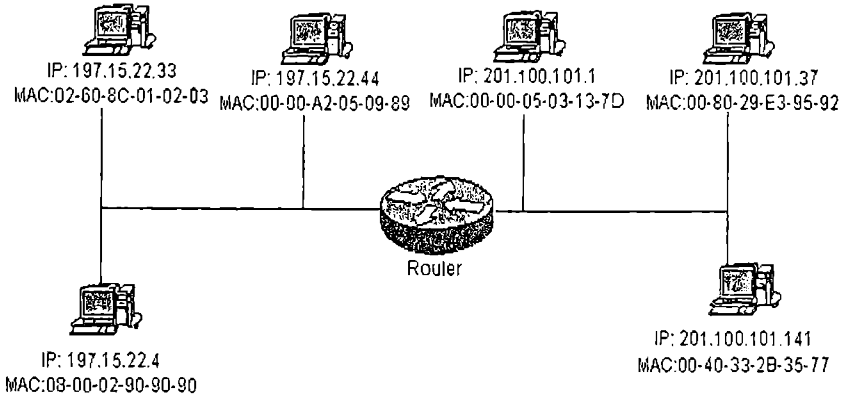


Figura 5.3.2. Cerere ARP către router

În aceste situaţii, staţia sursă lansează o cerere ARP. Routerul, care este conectat la aceeaşi reţea ca şi staţia sursă, preia cererea ARP şi răspunde staţiei respective. Acest răspuns conţine adresa MAC a unui router care nu face parte din reţeaua locală. Dacă cererea ARP pe care o lansează staţia sursă nu ar „trece" de graniţele reţelei locale, această staţie nu ar putea obţine informaţii despre adresele destinatarului.

Să recapitulăm puţin. Avem două staţii (sursă şi destinaţie) aflate în reţele diferite (ceea ce înseamnă că identificatorii de reţea sînt diferiţi). Staţia sursă nu cunoaşte adresa MAC a staţiei destinaţie. Prin urmare, sursa face apel la serviciile unui router pentru a putea transmite date destinatarului. Routerul care oferă astfel de servicii este denumit *default gateway*.

Pentru a putea obţine serviciile mai sus-amintite, staţia sursă încapsulează datele cu adresa MAC a routerului. Adresa IP folosită în antetul datagramei IP este cea a staţiei destinatare, şi nu cea routerului. De ce? Pentru că staţia sursă doreşte să transmită datele unei alte staţii, şi nu routerului. Cînd routerul recepţionează datele, extrage şi analizează informaţiile specifice nivelului 2, restul datelor fiind transferate nivelului reţea. Aici este examinată adresa IP destinaţie. Routerul compară această adresă cu informaţiile conţinute în tabelele de rutare. Dacă găseşte o corespondenţă, adresa IP-adresă MAC şi destinatarul face parte din una dintre reţelele la care este ataşat, routerul încapsulează datele cu noua adresă MAC şi le transmite destinaţiei.

Dacă, în schimb, în tabelele de rutare nu se regăsesc informaţii cu privire la destinatarul pachetului, routerul caută adresa MAC a unui alt router şi îi transferă acestuia datele. Acest tip de rutare este cunoscut şi sub denumirea de rutare indirectă.

Cum „învaţă" un router atîtea informaţii? Prin două metode: *statică* şi *dinamică*. Spus în cîteva cuvinte, aceste lucruri ar suna cam aşa: dacă informaţiile din tabelele de rutare trebuie scrise de „cineva", se spune că este vorba de rutare statică; dacă routerul poate învăţa singur cum se va face rutarea, se spune că este o rutare dinamică.

Cînd se foloseşte una sau alta dintre cele două variante? Dacă administratorul de reţea doreşte să controleze cu „mînuţele" lui care vor fi căile folosite de router pentru a transmite pachetele la destinaţie sau dacă orice pachet va fi transmis pe un singur drum la destinaţie, se va folosi rutarea statică.

5.4. ICMP - protocolul mesajelor de control[1]

Spuneam că în cadrul IP, unitatea de bază folosită în transferul datelor o reprezintă datagrama IP. Procesarea acestor datagrame se face la nivelul software-ului. Altfel spus, conţinutul şi formatul unei datagrame nu sînt dependente de hardware.

Trebuie menţionat că alte protocoale de comunicaţie au propriul format pentru datagrame. Datagrama IP este specifică IP.

O altă componentă majoră a IP este **ICMP (Internet Control Message Protocol)**. Acest protocol este folosit de echipamentele dintr-o reţea pentru a raporta sursei problemele care au apărut în timpul transmiterii unui mesaj. Au fost definite mai multe astfel de mesaje, cele mai importante fiind cele care urmează:

1. Descris în RFC792.

Destination unrechable (Destinaţie inaccesibilă) este mesajul folosit atunci cînd subreţeaua sau un router nu pot localiza destinaţia unei datagrame sau cînd un pachet cu bitul DF nu poate fi livrat, deoarece trebuie să tranziteze o reţea cu pachete mici.

Time exceeded (Timp depăşit) este mesajul transmis cînd un pachet este eliminat ca urmare a ajungerii contorului său la zero. De obicei, prin acest mesaj se identifică blocajele din reţea.

Mesajul *Parameter problem* (Problemă de parametru) arată o valoare nepermisă într-un cîmp din antetul datagramei.

Prin *Redirect* (Redirectare), routerul avertizează că un pachet pare a fi dirijat pe un traseu greşit.

O caracteristică a ICMP o reprezintă *echo-request/echo-reply*, prin care se testează dacă un pachet poate să ajungă la destinaţie prin „pinguirea" acesteia. Trebuie să menţionăm că mesajele de tipul *destination unreachable* au la rîndul lor mai multe subcategorii.

CAPITOLUL 6

Nivelurile sesiune şi prezentare

6.1. Cîteva consideraţii generale despre o sesiune

Nivelul sesiune este cel care coordonează aplicaţiile ce interacţionează cînd două calculatoare comunică între ele.

Comunicarea între două calculatoare implică derularea unor mini-conversaţii pentru a se asigura că cele două calculatoare pot efectiv comunica. În timpul acestor mini-conversaţii fiecare dintre participanţi joacă un rol dublu: ca şi în cazul unui client, pot să ceară la un moment dat un serviciu, dar, ca şi în cazul unui server, pot să ofere un serviciu. Procesul prin care se determină ce rol joacă, la un moment dat, unul dintre calculatoare se numeşte controlul dialogului. Tot nivelul sesiune este cel care stabileşte, gestionează şi încheie sesiunile de lucru între aplicaţii.

Nivelul sesiune este cel care decide cînd are loc o comunicare în ambele sensuri simultan sau cînd are loc o comunicare în ambele sensuri alternativ (controlul dialogului). Dacă se permite o comunicare în ambele sensuri simultan, nivelul sesiune devine mai puţin activ în ceea ce priveşte gestionarea conversaţiei şi permite celorlalte niveluri ale celor două calculatoare să controleze întregul proces. În acest caz este posibil să apară coliziuni în cadrul acestui nivel, coliziuni care sînt diferite de coliziunile care apar la nivel fizic.

Coliziunile de la nivelul sesiune se manifestă doar sub forma a două mesaje transmise unul către celălalt şi care creează confuzie fie la nivelul unui calculator, fie în ambele. Dacă aceste coliziuni nu sînt tolerate, controlul dialogului apelează la o comunicare în ambele sensuri alternativ. În acest caz se foloseşte un jeton specific nivelului sesiune, prin care cele două calculatoare stabilesc ordinea în comunicare (similar cu jetonul de la nivelul 2). În acest moment se pot pune două întrebări: Cum se realizează separarea dialogului în timpul comunicării? Cum se sincronizează comunicarea?

Separarea dialogului face apel la punctele de control (*checkpoint*). Aceste puncte acţionează similar cu momentul în care se declanşează AutoSave-ul Word-ului în timpul tehnoredactării. Ele separă părţile dialogului dintre cele două calculatoare. Separarea dialogului se referă la iniţierea ordinii, gestionarea şi terminarea comunicării.

În ceea ce priveşte sincronizarea comunicării, aceasta poate fi minoră sau majoră. Ce presupune sincronizarea minoră?

La momentul *t* (momentul declanşării *checkpoint*-ului), nivelul sesiune al unui calculator transmite un mesaj de sincronizare către calculatorul cu care dialoghează. În acest moment ambele calculatoare vor executa următoarele rutine:

- realizează copii de siguranţă pentru fişierele particulare;

- salvează setările reţelei ;
- salvează setările ceasului ;
- iau la cunoştinţă de terminarea conversaţiei.

Sincronizarea majoră este mult mai complexă şi implică mult mai multe etape.

Şi dacă tot am pomenit în acest curs de protocoale de nivel superior, protocoalele nivelului 5 pot fi identificate în timpul login-ului sau în cadrul unei aplicaţii : NFS (*Network File System*), SQL (*Structured Query Language*), RPC (*Remote Procedure Call*), X-Window System, ASP (*Apple Talk Session Protocol*), DNA (*Digital Network Architecture*), SCP (*Session Control Protocol*).

6.2. Prezentare

Nivelul prezentare este cel care răspunde de prezentarea datelor într-o formă pe care calculatorul sursă să o poată „înţelege". Acest nivel acţionează ca un traducător pentru echipamentele care comunică într-o reţea şi îndeplineşte trei funcţii principale :

- prezentarea datelor (sau formatul acestora) ;
- criptarea datelor ;
- compresia datelor.

După ce primeşte datele de la nivelul aplicaţie, dar înainte de a le transmite nivelului sesiune, nivelul prezentare execută una sau mai multe dintre funcţiile prezentate anterior. La destinaţie, nivelul prezentare preia datele de la nivelul sesiune, execută funcţiile necesare şi apoi transferă respectivele date nivelului aplicaţie.

Să presupunem că staţia pe care lucraţi vrea să comunice cu un mainframe. Sistemul vostru foloseşte codurile ASCII pentru reprezentarea caracterelor, în timp ce mainframe-ul foloseşte codurile EBCDIC. Traducerea informaţiilor dintr-un cod în altul este realizată cu ajutorul nivelului 6.

Dincolo de reprezentarea caracterelor, standardele nivelului 6 vizează şi modalităţile de prezentare a imaginilor grafice :

- PICT - format pentru imagini, utilizat pentru transferul imaginilor grafice QuicDraw între programele sistemelor MAC ;
- TIFF - format pentru imagini bit-map cu rezoluţie mare ;
- JPEG - formatul *joint photographic experts group*.

Alte cerinţe ale nivelului 6 se referă la formatul de prezentare a sunetelor şi filmelor :

- MIDI - pentru sunet digital (*Musical Instrument Digital Interface*) ;
- MPEG - standard pentru compresia şi codificarea filmelor video pe suport CD etc. (*Motion Picture Experts Group*) ;
- QuickTime - standardul pentru pentru lucrul cu fişiere audio-video pe maşini MAC (diferenţă faţă de *QuickTime for Windows*).

Codurile ASCII şi EBCDIC sînt folosite pentru formatarea textelor. Fişierele text bazate pe coduri ASCII nu fac apel la comenzi ultra-sofisticate. Gîndiţi-vă la Notepad.

Este destul de simplu de scris un text cu acest utilitar. EBCDIC este un cod similar cu ASCII, singura diferenţă majoră constînd în tipul calculatorului pentru care sînt dedicate. Majoritatea fişierelor realizate cu ajutorul unui editor de texte au extensia .txt.

Un alt format destul de utilizat în cazul fişierelor este formatul *binary* (binar). În aceste fişiere datele sînt codificate astfel încît nu pot fi citite decît cu aplicaţii specifice. Un exemplu de program care foloseşte fişiere binare este FTP-ul.

Aminteam, mai înainte, de cîteva formate folosite în cazul fişierelor grafice. În Internet, cele mai folosite formate de fişiere pentru afişarea imaginilor sînt : GIF (*Graphic Interchange Format*) şi JPEG.

În categoria fişierelor binare intră şi formatul de fişiere multimedia : capabile să memoreze sunete şi imagini la un loc. Fişierele audio pot fi ascultate prin două metode : fie mai întîi sînt descărcate şi apoi ascultate, fie sînt ascultate în timp ce sînt descărcate (*streaming audio*). Windows-ul foloseşte formatul WAV pentru sunet şi AVI pentru imaginile animate. Pentru fişierele video, cele mai cunoscute formate sînt variantele MPEG.

Un alt format de fişiere, format ce acţionează ca un set de reguli pentru afişarea şi gestiunea documentelor de către browsere, este *markup language*. HTML (*HyperText Markup Language*) este limbajul (nu de programare) folosit în Internet pentru afişarea paginilor.

Folosind un soft specializat, la nivelul 6 se poate realiza şi criptarea datelor. De ce este nevoie de criptare? Pentru a proteja informaţiile în timpul transmiterii lor prin reţea. Majoritatea tranzacţiilor financiare ce se derulează prin Internet fac apel la criptare. De cele mai multe ori, o astfel de aplicaţie foloseşte o cheie de criptare pentru a codifica datele într-o nouă formă şi o cheie de decriptare pentru a le aduce în forma iniţială.

Tot nivelul prezentare este cel care răspunde şi de compresia fişierelor, o tehnică prin care se reduce mărimea lor folosind algoritmi destul de complecşi.

CAPITOLUL 7

Nivelul aplicaţie

Nivelul aplicaţie este cel mai apropiat de utilizatorul calculatorului. Este nivelul responsabil cu identificarea partenerilor disponibili să comunice, sincronizarea aplicaţiilor, stabilirea procedurilor pentru recuperarea datelor şi controlează integritatea acestora.
Este singurul nivel care nu oferă servicii celorlalte niveluri ale modelului OSI.

7.1. DNS - Domain Name System[1]

Cînd am prezentat nivelul reţea spuneam că foloseşte o schemă de adresare ierarhizată. Programele însă fac referire destul de rar la sistemele gazdă prin adresa lor IP. De cele mai multe ori se utilizează şiruri ASCII de genul : adim@yahoo.com, www.feaa.uaic.ro sau www.crap.ro. Chiar şi în această situaţie Internetul ştie numai de adresele binare despre care am discutat deja. Prin urmare, a fost nevoie de un mecanism care să convertească şirurile ASCII în adrese binare. Pentru majoritatea dintre noi este mult mai uşor de memorat un nume decît o adresă binară. Din acest motiv, proiectanţii Internetului au creat DNS (Sistemul Numelor de Domenii) care permite referirea calculatoarelor gazdă cu ajutorul numelor.

DNS este, practic, un soft care transformă numele (feaa.uaic.ro) în adresă IP şi invers. Pentru a face o astfel de transformare, DNS are nevoie de cîteva informaţii. Aceste informaţii sînt stocate pe mai multe calculatoare din Internet (servere DNS). În fond, DNS este un exemplu tipic de baze de date distribuite. O bază de date distribuită poate fi văzută ca o sumă de fişiere memorate pe calculatoare diferite din Internet - localizate în spaţii geografice diferite. Softul pentru baza de date distribuită gestionează şi controlează întreaga colecţie de date ca pe o singură bază de date.

DNS este alcătuit din trei mari componente :

- Spaţiul numelor de domeniu,
- Servere de nume,
- Resolvere.

Spaţiul numelor de domenii reprezintă informaţia conţinută în baza de date distribuită din Internet. Putem să ne imaginăm această informaţie ca o structură arborescentă :

- arpa - este un domeniu Internet special, care transformă adresele IP în nume ;

1. Descris în RFC1034,1035.

- grupul generic sau al organizaţiilor - are etichete de domeniu compuse din trei caractere (com, edu, gov, mil);
- grupul geografic al ţărilor - are etichete de domeniu compuse din 2 caractere (us, ro, fr).

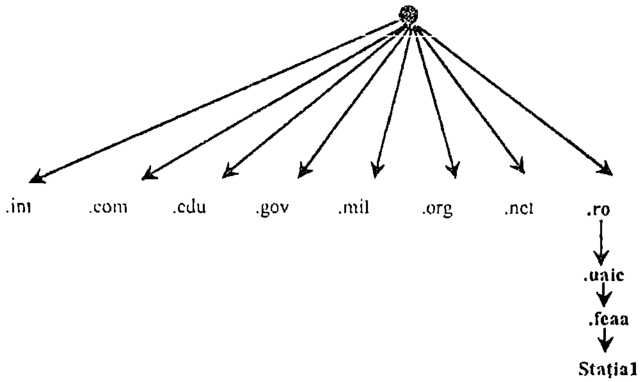


Figura 7.1.1. Structura DNS

Internet Assigned Numbers Authority (IANA)[1] este organismul care administrează la nivel mondial numele de domenii. La nivel conceptual, Internetul este divizat în domenii de nivel superior care, la rîndul lor, sînt divizate în subdomenii etc.

Componentele unui nume pot avea maximum 64 de caractere, iar întreaga cale nu poate depăşi 255 de caractere. Numele de domenii ar trebui să conţină doar litere, deşi în practică se întîlnesc situaţii care nu respectă această cerinţă (atunci cînd se doreşte ca site-ul să fie mai uşor de regăsit de către motoarele de căutare se introduc şi cifre). O astfel de situaţie poate crea probleme aplicaţiilor care analizează doar primul caracter al unei adrese pentru a identifica DNS-ul căreia aparţine.

Fiecare domeniu controlează maniera de alocare a subdomeniilor sale, motiv pentru care atunci cînd se creează un nou domeniu, se cere permisiunea domeniului în care va fi inclus.

Serverele de nume sînt programe server care stochează informaţia DNS şi răspund cererilor adresate de alte programe. Un server de nume nu trebuie să ştie adresele celorlalte servere de nume din DNS. În schimb, trebuie să ştie cum să contacteze serverele de nume rădăcină, care, la rîndul lor, trebuie să ştie numele şi adresele IP ale tuturor serverelor de nume de nivel doi. Arborele serverelor de nume este foarte larg şi cu foarte puţine niveluri. Deci, serverul nu trebuie să transmită cererea la prea multe servere.

1. Vezi www.iona.org.

Domeniile de responsabilitate poartă denumirea de *zone*. Organizația responsabilă pentru o anumită zonă poate divide mai departe zona, fragmentînd-o pînă cînd o singură persoană poate gestiona alocarea numelor. Această persoană este numită, de obicei, administrator DNS.

Deoarece serviciile de căutare DNS sînt operații critice (dacă un program nu poate obține adresa IP căutată, nu poate realiza conexiunea dorită), Internet a impus, pentru fiecare zonă, un server DNS primar și unul sau mai multe servere secundare. În general, serverele secundare conțin aceeași informație ca serverul primar. Ele sînt folosite pentru a crea „copii de siguranță", în cazul în care serverul primar se defectează sau este supraîncărcat cu cereri.

Un server de nume primar stochează informația DNS local în fișiere speciale. Un server de nume secundar preia datele de la serverul primar al zonei, printr-un proces care poartă numele de *transfer zonal*. În general, un server secundar interoghează serverul primar o dată la cîteva ore.

Resolverele sînt programe care extrag informațiile din serverele de nume, ca răspuns la cererile unor clienți. Un client contactează serverul de nume pentru zona din care face parte. Serverul examinează cererea pentru a determina dacă are autoritate pentru domeniul specificat. În caz afirmativ, se face transformarea numelui în adresa IP și se trimite răspunsul înapoi la client. În cazul în care serverul nu poate face transformarea direct, răspunsul depinde de tipul cererii trimise de client. Un client poate cere o transformare a numelor în două moduri:

- *cu rezolvare recursivă* – serverul va contacta la rîndul lui un alt server de nume, de obicei de pe un nivel superior din arborele serverelor de nume. Acesta, la rîndul lui, va examina cererea și dacă nu poate să facă transformarea, va contacta un alt server. Și tot așa, pînă cînd va fi contactat un server care poate rezolva această cerere;
- *cu rezolvare iterativă* – serverul va comunica clientului ce server să contacteze mai departe. Clientul va adresa o cerere acestui server, trimis de serverul zonal, și tot așa mai departe pînă cînd cererea va ajunge la un server care va face transformarea. Cînd un server recepționează o cerere cu rezolvare iterativă și nu poate traduce numele de domeniu, acesta va transmite clientului ce server să contacteze mai departe.

7.2. SNMP – Protocolul simplu pentru administrarea rețelelor[1]

SNMP (*Simple Network Management Protocol*) este protocolul nivelului aplicație proiectat pentru a oferi posibilitatea schimbului de informații de administrare între dispozitivele unei rețele. Parte a suitei TCP/IP, SNMP permite administratorilor de rețea să gestioneze performanțele unei rețele, să identifice și să rezolve problemele care apar precum și să planifice dezvoltările ulterioare ale rețelei.

1. Descris în RFC1157.

În termeni simpli, despre SNMP se poate spune că este un protocol asimetric de tip *request-reply* care schimbă informaţii între o staţie de administrare şi un agent. Agentul nu este altceva decît dispozitivul care se doreşte a fi administrat.

SNMP este alcătuit din trei elemente de bază:

- *Management stations* - staţii de administrare;
- *Agent* - noduri administrate;
- *Management Information Base (MIB)* - informaţii de administrare.

Staţiile de administrare (NMS - *Network Management Station*) pot fi oricare dintre calculatoarele reţelei pe care se execută programele de administrare. Acestea comunică cu agenţii prin intermediul SNMP, trimiţînd comenzi şi primind în schimb răspunsuri. Dialogul dintre aceste două componente are la bază MIB care reprezintă o colecţie de informaţii organizate ierarhic, ce descriu obiectele care sînt administrate.

Protocolul SNMP permite staţiei de administrare să interogheze un agent cu privire la starea obiectelor locale şi să le modifice dacă este necesar. Există situaţii în care dacă un agent observă că s-a produs un eveniment, raportează către toate staţiile de administrare (*trap SNMP*). Staţia de administrare interoghează apoi agentul pentru a afla detalii despre evenimentul care a avut loc.

În cazul în care în reţea există dispozitive care nu sînt capabile să ruleze un agent SNMP, se face apel la un *proxy agent* (agent intermediar) care va prelua sarcinile agentului clasic.

Spuneam că nucleul SNMP-ului îl reprezintă baza de informaţii. Pentru a se asigura comunicarea între diferitele dispozitive ale unei reţele, este esenţial ca obiectele să aibă o definiţie standardizată, independentă de producătorul respectivului echipament.

Limbajul standard folosit de SNMP pentru definirea obiectelor şi a regulilor de codificare se numeşte **ASN.1 (Abstract Syntax Notation One) - notaţia sintactică abstractă unu.**

7.3. Poşta electronică

Pe la începuturile sale, Internetul de astăzi a avut patru aplicaţii principale:

- poşta electronică;
- ştiri;
- conectarea la distanţă;
- transferul de fişiere.

Poşta electronică nu este o aplicaţie chiar atît de simplă pe cît pare. E drept că puteţi să o folosiţi şi fără să ştiţi cele ce urmează!

Pentru a putea transmite un mesaj prin intermediul poştei electronice este nevoie de cîteva ingrediente: un calculator, o conexiune la reţea (modem, de exemplu), un program care permite utilizarea acestui serviciu de Internet, o conexiune la Internet (oferită de un provider - ISP - sau de un serviciu online) şi o banală adresa de e-mail.

Mesajul pe care îl transmiteţi este preluat în reţeaua Internet de către un server şi apoi livrat calculatorului menţionat în adresa de e-mail.

Cum este alcătuită o adresă de e-mail? Adresa de poştă electronică este o adresă Internet formată din două părţi, despărţite de caracterul @:

- prima parte a adresei reprezintă numele de conectare al persoanei căreia îi este destinat mesajul (ID_user);
- a doua parte reprezintă denumirea domeniului din care face parte persoana (identifică nodul destinaţie - adresa_nod);

Dacă aveţi instalat un browser ca Netscape Navigator/Communicator sau Microsoft Internet Explorer, aveţi şi aplicaţiile necesare pentru e-mail. Există şi altele nu numai cele ale rivalilor amintiţi: Pine (pentru Unix), EudoraPro, America Online (AOL), HotCast, Calypso, Messenger.

Pentru a primi sau a trimite un mesaj, calculatorul trebuie însă să comunice cu un server de e-mail, folosind un anumit protocol de livrare. Acest protocol se stabileşte, de obicei, în momentul configurării softului de e-mail.

POP - Post Office Protocol (protocol de poştă), este un protocol simplu utilizat pentru aducerea mesajelor dintr-o cutie poştală aflată la distanţă. Scopul acestui protocol este de a aduce poşta electronică de la distanţă şi de a o depozita pe calculatorul local al utilizatorului, pentru a fi citită mai tîrziu. Este cel mai vechi protocol, prima versiune a fost definitivată în anul 1984, ajungîndu-se în prezent la POP3.

IMAP - Interactive Mail Access Protocol (protocol interactiv de acces la poştă), este un protocol care a fost proiectat pentru a ajuta utilizatorii care folosesc mai multe calculatoare (un calculator la birou, un calculator acasă sau un notebook). În acest caz, server-ul de e-mail păstrează un depozit central de mesaje la care accesul poate fi realizat de pe orice calculator. În comparaţie cu protocolul POP3, IMAP nu copiază poşta electronică pe calculatorul personal al utilizatorului.

DMSP - Distributed Mail System Protocol (protocol distribuit pentru sistemul de poştă), este un protocol care permite utilizatorilor să aducă poşta electronică de pe serverul de e-mail pe un calculator şi apoi să se deconecteze de la server.

Cînd se alege un client de e-mail, trebuie avute în vedere următoarele:

- ce standarde suportă: IMAP4 sau POP3?;
- capabilitatea de lucru cu conturi de e-mail multiple;
- posibilitatea de a aduce de pe server doar mesajele dorite, celelalte fiind eliminate prin filtre;
- posibilitatea de arhivare a mail-urilor, precum şi importul şi exportul textelor;
- ergonomia (interfaţa cu utilizatorul, modul de explicitare a erorilor intervenite, documentaţia);
- funcţionalitatea: în ce măsură clientul de e-mail îndeplineşte şi atinge cerinţele utilizatorului, prin opţiunile puse la dispoziţie;
- resurse necesare sistemului pentru fiecare aplicaţie în parte, pentru a rula optim şi fără întreruperi;
- dacă suportă format HTML.

Toate programele de e-mail funcţionează pe baza unor protocoale de comunicaţie, în afara celor de livrare, care asigură accesul la serverul de poştă electronică precum şi livrarea mesajelor. Cele mai cunoscute standarde de poştă electronică (protocoalele de acces) sînt:

ISO – localizează activităţile de procesare a mesajelor electronice la nivelul 7 al modelului OSI. Acesta permite ca reţele diferite să poată comunica, indiferent de deosebirile existente între sistemele de operare folosite ;

SMTP – Simple Mail Transfer Protocol (protocol simplu de transfer de poştă) este un protocol pentru transferul mesajelor între două calculatoare din reţea aflate la distanţă. Este un protocol folosit în Internet şi face parte din stiva de protocoale TCP/IP. Funcţionează împreună cu programe de poştă electronică, oferind atît pentru client, cît şi pentru server funcţii de transmitere şi recepţionare a mesajelor e-mail.

MHS – Message Handlig Service este un standard popularizat de către firma Novell. Serverul MHS transmite mesaje între calculatoare care folosesc sisteme e-mail diferite.

MIME – Multipurpose Internet Mail Extensions (extensii de poştă cu scop multiplu) este un protocol prin intermediul căruia se pot transmite şi recepţiona şi mesaje non ASCII : imagini, audio, video etc.

7.4. File Transfer Protocol[1] (Protocol pentru transferul fişierelor)

FTP este protocolul care oferă facilităţi pentru transferul fişierelor pe sau de pe un calculator din reţea. De multe ori, pentru această acţiune utilizatorul este nevoit să se autentifice pe calculatorul de pe care doreşte să încarce/descarce fişiere. Facilitatea cunoscută sub numele de *anonymous ftp* lucrează cu un cont public implementat pe calculatorul gazdă, numit *guest*.

O sesiune ftp presupune interacţiunea a cinci componente soft :

Interfaţa utilizator	Oferă interfaţa de lucru şi gestionează interpretorul protocolului client.
PI Client	Interpretorul protocolului client. Un interpretor este cel care transmite comenzile către interpretorul serverului aflat la distanţă şi gestionează transferul datelor către client.
PI Server	Interpretorul protocolului server răspunde comenzilor lansate de client şi gestionează transferul datelor de pe server.
Client DTP	Procesul de transfer al datelor către client răspunde de comunicarea cu procesul serverului şi fişierele locale.
Server DTP	Procesul de transfer al datelor de pe server răspunde de comunicarea cu procesul client şi fişierele aflate la distanţă.

În timpul unei sesiuni ftp se realizează două conexiuni separate : una între PI-uri şi una între DTP-uri. Prima este cunoscută sub denumirea de **conexiune de control**, iar cea de a doua se numeşte **conexiunea datelor**.

Cînd funcţionează, un server ftp „ascultă" portul 21 pentru a vedea dacă există cereri de conexiune. Alegerea portului pentru conexiunea datelor depinde de comenzile transmise prin conexiunea de control. De obicei, clientul transmite un mesaj de control prin care se indică numărul portului de pe maşina client pe care se acceptă o cerere de conexiune a datelor.

1. Descris în RFC 959.

Folosirea celor două tipuri de conexiuni oferă avantajul selectării corespunzătoare a serviciilor : întîrziere minimă pentru conexiunea de control şi productivitate (*throughput*) maximă pentru conexiunea datelor.

În general, cînd se iniţiază un transfer prin ftp, trebuie precizate următoarele aspecte :

1. Tipul fişierului.

Se specifică maniera în care datele conţinute de un fişier vor fi aduse într-un format transportabil prin reţea :

- fişiere ASCII - calculatorul care transmite fişierul îl converteşte din formatul local text în format ASCII ;
- fişiere EBCDIC - similar cu ASCII ;
- fişiere binare (*binary*) - fişierul este transmis exact cum este memorat pe calculatorul sursă şi memorat la fel pe calculatorul destinaţie ;
- fişiere locale - folosite în mediile în care cel ce transmite precizează numărul de biţi/byte.

2. *Controlul formatului* - se referă la fişierele text care sînt transferate direct către o imprimantă :

- *No printing controls* (*default*) ;
- *telnet printing controls* ;
- *fortran printing controls*.

3. *Structura* - fişierele pot să-şi păstreze structura internă în timpul transmisiei. De acest lucru se ocupă procesul pentru transferul datelor (DTP). Există trei posibilităţi :

- Structura fişierului - fişierul este văzut ca un flux continuu de bytes, fără o structură internă.
- Structura înregistrării - fişierul este structurat ca o serie de înregistrări (valabil în cazul fişierelor text).
- Structura paginii (structură bloc) - fiecare pagină este numerotată pentru a putea fi transmisă în orice ordine.

4. *Modul de transmitere* implică trei posibilităţi :

- Stream (în flux) - fişierul este transferat într-o serie de bytes.
- Bloc - fişierul este transferat bloc cu bloc, fiecare cu un header.
- Compresat - se foloseşte o schemă de comprimare a secvenţelor de bytes identici.

În timpul unui transfer prin ftp nu există nici un mecanism de negociere a transmisiei.

7.5. World Wide Web

Conceptul care a stat la baza WWW este **hypertextul**.

Prin hypertext se înţelege o colecţie de documente unite între ele prin legături (*link*) ce permit parcurgerea acestora bidirecţional.

HTTP este acronimul pentru **HyperText Transfer Protocol** sau protocolul ce stabileşte regulile de transfer al documentelor hypermedia. Aplicaţiile care folosesc acest protocol sînt considerate entităţi abstracte din punctul de vedere al protocolului. Ele trebuie să poată formula cereri şi/sau recepţiona răspunsuri (modelul client-server).

Unul dintre conceptele de bază este cel de **resursă** şi desemnează un calculator, o bază de date, un document sau, spus la modul general, *un serviciu*. Resursa trebuie să poată fi referită corect şi fără echivoc. Pentru referirea unei resurse în Internet, se foloseşte termenul generic **URI - Uniform Resource Identifier.** Dacă se face referire la o locaţie, spunem că avem de a face cu un **URL - Universal Resource Locator.** Dacă se face referire la un nume, avem de-a face cu un **URN - Universal Resource Name.**

Protocolul se bazează pe paradigma cerere/răspuns. Clientul cere accesul la o resursă, aceasta fiind identificată prin URI, iar serverul răspunde printr-o linie de stare (conţine, printre altele, un cod de succes sau eroare şi, în primul caz, urmează datele cerute).

Adresarea unei resurse în Internet se face prin construcţii de forma:

protocol: //[serviciu].nume_dns[.nume_local/cale/subcale/nume_document

Serverul care răspunde cererilor privitoare la documente hypermedia se numeşte server WWW: „cunoaşte" protocolul http şi oferă serviciul www.

Partea a II-a

Proiectarea reţelelor de calculatoare

CAPITOLUL 8

Cablarea structurată a unei reţele de calculatoare

Ce reprezintă cablarea structurată? În cuvinte simple, reprezintă o arhitectură pentru comunicaţiile prin cablu, specificată de către comitetul EIA/TIA TR42[1] şi folosită, în mod voluntar, ca standard de către producătorii de echipamente.

Un sistem de cablare structurată include mediile de transmisie şi hardware-ul asociat cu scopul de a furniza o infrastructură de comunicaţii cuprinzătoare. Această infrastructură nu trebuie să fie dependentă de un anumit dispozitiv. Mai mult, un sistem de cablare structurată începe din punctul în care se termină infrastructura furnizorului de servicii. Chiar dacă respectă aceeaşi metodologie, orice sistem de cablare structurată este unic în felul său din mai multe motive:

- structura arhitecturală a clădirii în care se realizează instalarea;
- produsele folosite;
- funcţia îndeplinită de sistemul de comunicaţii;
- configuraţia echipamentelor;
- cerinţele şi limitările clientului.

8.1. Standardul ANSI/TIA/EIA 568

Conform acestui standard, un sistem de cablare structurată cuprinde şase elemente:

- cablarea orizontală;
- cablarea principală (coloana vertebrală a reţelei[2]);
- zona (spaţiul) de lucru (birourile);
- panoul pentru telecomunicaţii (rack-ul sau cabinetul în care sînt depozitate echipamentele de reţea);
- sala echipamentelor;
- facilităţile de acces.

---

1. Electronics Industry Alliance/Telecommunications Industry Association – asociaţie care asigură în mod voluntar standardele pentru interoperabilitatea echipamentelor de comunicaţie produse de membrii săi.
2. Backbone – partea de reţea care sprijină traficul principal al reţelei.

Cablarea orizontală

Acest subsistem acoperă suprafața cuprinsă între priza din zona de lucru (birou) și panoul pentru telecomunicații. Cablarea orizontală trebuie configurată într-o topologie stea, fiecare rack din zonele de lucru fiind conectat printr-o conexiune încrucișată la sala cu echipamente pentru telecomunicații.

Distanța maximă a unui segment va fi de 90 metri la care se adaugă cablurile din zona de lucru cu o lungime de maximum 10 metri. Pe lîngă cablurile din acest subsistem mai fac parte : conectorii pentru telecomunicații (prizele), conectorii și cablurile din interiorul rack-ului.

Mediile de transmisie recunoscute de standard sînt :

- cablul UTP de 100 ohm ;

- cablul STP de 150 ohm ;

- fibra optică multimod (62.5/125 μm).

În fiecare zonă de lucru trebuie să existe o priză cu două module :

- un modul pentru cablu UTP cel puțin categoria 3, de 100 ohm ;
- un modul pentru unul dintre mediile de transmisie prezentate mai sus.

Cerințele legate de montaj trebuie să respecte specificațiile standardului ANSI/TIA/EIA-607.

*Cablarea principală (*backbone*)*

Backbone-ul rețelei suportă cantitatea cea mai mare de trafic și interconectează între ele cabinetele cu echipamente, sălile cu echipamente sau facilitățile de acces. În acest caz, topologia este stea ierarhică și poate fi completată, în funcție de situație, și cu topologii inel sau magistrală.

Distanțele maxime admise[1] pentru mediile de transmisie sînt :

Mediu de transmisie	Distanță maximă admisă pentru backbone
100 ohm UTP (24 or 22 AWG)	800 metri pentru voce, 90 metri pentru date
150 ohm STP	90 metri pentru date
Fibră optică multimod 62.5/125 μm	2000 metri
Fibră optică single-mode 8.3/125 μm	3000 metri

Patch cordurile nodului central și cele din nodurile secundare nu ar trebui să depășească 20 de metri. Cablurile pentru conectarea celorlalte echipamente nu ar trebui să depășească 30 de metri.

1. Aceste distanțe sînt dependente de aplicațiile implementate.

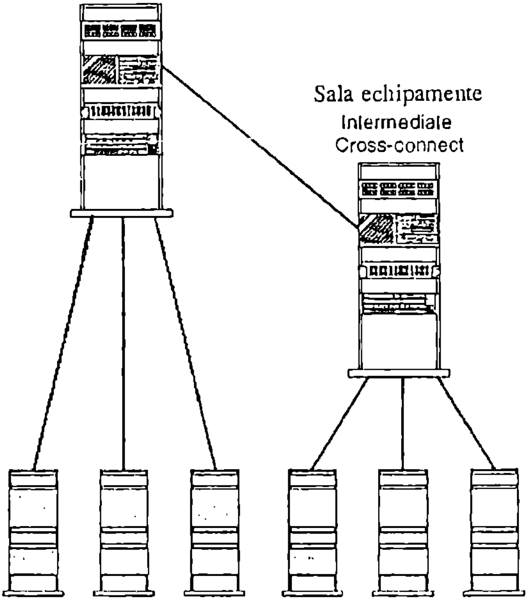


Figura 8.1.1. Topologie star cu două niveluri interconectate
(Sursa : http ://faculty.petra.ac.id/resmana/jarkom/structured_cabling/tiabook2.htm)

Zona de lucru

Această componentă se întinde de la priza pentru comunicații pînă la stația de lucru sau alt echipament de lucru. Este zona în care se regăsesc utilizatorii rețelei. Cablarea în acest caz trebuie să permită adaptarea rapidă la modificările care intervin : adăugarea unor stații noi, de exemplu.

Componentele acestui subsistem includ :

- stațiile de lucru, terminalele, telefoanele etc ;
- cablurile de prelungire (patch cablurile) ;
- diferite adaptoare.

Panoul (cabinetul) pentru telecomunicații

Panoul pentru telecomunicații reprezintă zona în care sînt concentrate echipamentele prin care se interconectează mediile de transmisie : terminatorii mecanici și sistemul de cabluri cross sau backbone. Specificațiile tehnice ale acestui panou sînt definite prin standardul EIA/TIA 569A.

Sala echipamentelor

Specificaţiile pentru proiectarea sălii echipamentelor sînt prezentate în standardul EIA/TIA 569A. O astfel de sală poate prezenta oricare dintre facilităţile unui panou pentru telecomunicaţii.

Facilităţile de acces

Această componentă se referă la punctul de interacţiune dintre cablurile din interiorul clădirii şi cele ale backbone-ului. Cerinţele fizice sînt definite prin EIA/TIA 569A. Această zonă trebuie să fie, în fapt, o încăpere sigură de unde încetează responsabilităţile furnizorului de servicii şi intră în acţiune proprietarul reţelei.

Specificaţii în legătură cu acest subiect găsiţi şi la *http://cablingdb.com/GlossaryPages.*

8.2. Instalarea cablurilor

Chiar dacă am făcut o prezentare generală a acestui mediu de transmisie, vom reveni acum cu aspectele legate de instalarea sa. Cele mai multe probleme legate de reţele apar din cauza cablurilor: performanţele reţelei sînt strîns legate de cele ale cablurilor.

Instalarea reţelei trebuie făcută pe baza unei documentaţii şi a unui proiect iniţial, care să ţină cont de aspectele prezentate pînă acum. Vom reveni asupra instrumentelor disponibile pentru proiectare şi documentare.

Majoritatea cutiilor în care este „împachetat" cablul sînt proiectate astfel încît desfăşurarea acestuia să fie cît mai uşoară. O astfel de cutie conţine aproximativ 300 de metri de cablu pe care este marcată distanţa din metru în metru (sau în picioare). De fiecare dată cînd folosiţi cablu dintr-o cutie, notaţi pe aceasta numărul de metri utilizaţi. Veţi şti astfel, în orice moment, cît cablu aveţi la dispoziţie pentru o lucrare.

O dată extras cablul din cutie, marcaţi pe el portul sau locaţia în care îl amplasaţi.

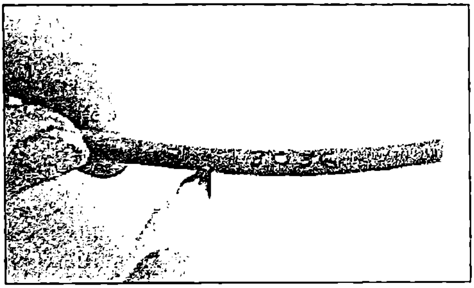


Figura 8.2.1. Marcarea cablurilor

Evitați astfel multe dintre neplăcerile ulterioare.

Perechile torsadate din cablul UTP au pe lîngă culori și cifre după cum urmează:

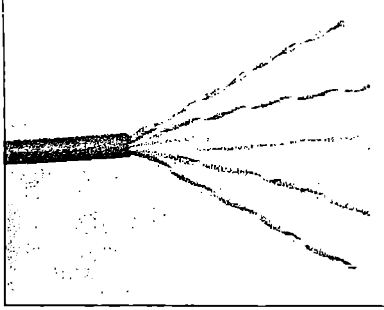


Figura 8.2.2. Structura cablului UTP

Este important de știut cifra corespunzătoare unei perechi pentru că un tester[1] pentru cabluri raportează întotdeauna perechea cu probleme, și nu culoarea acesteia. De cele mai multe ori, în depanarea cablurilor se face apel la un astfel de instrument, care în funcție de performanțe, pe lîngă perechea cu probleme, poate calcula latența pe un segment sau realizează harta cablurilor dintr-o zonă.

EIA/TIA 568B Pin#	Perechea #	Funcția	Culoarea firului	Ethernet 10/100 Base-T	Ethernet 100 Base-TX și 1000 Base-T ?
1	2	Transmite	Alb- portocaliu	Da	Da
2	2	Recepționează	Portocaliu	Da	Da
3	3	Transmite	Alb-verde	Da	Da
4	1	Nu se folosește	Albastru	Nu	Da
5	1	Nu se folosește	Alb-albastru	Nu	Da
6	3	Recepționează	Verde	Da	Da
7	4	Nu se folosește	Alb-maro	Nu	Da
8	4	Nu se folosește	Maro	Nu	Da

În jack-ul RJ 45, perechile sînt dispuse după cum urmează:

1. Vă recomandăm echipamentele de la Fluke, seria *Micro* (www.fluke.com).

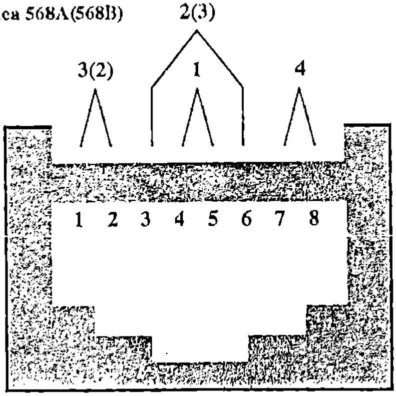


Figura 8.2.3. Ordinea perechilor

Secvența de culori pentru realizarea conexiunilor este următoarea:

- conexiune directă (conectare standard):

- conexiune inversată (crossover):

Vom detalia aceste aspecte deoarece nu toată lumea își permite să cumpere cablurile gata pregătite de pe piață.

Cablul prin care se conectează porturile din interiorul unui panou sau un echipament la o priză din zona de lucru se numește *patchcord*. Pentru realizarea sa este nevoie de cablul propriu-zis, conectori RJ45, protectori pentru aceste mufe și un cleşte de sertizat.

Cablarea unui patchcord se poate face standard, dacă se dorește interconectarea calculatoarelor la prizele de rețea sau la hub-uri/switch-uri, sau inversat, dacă se dorește interconectarea switch-urilor, de exemplu.

Manufacturarea propriu-zisă a cablului presupune înlăturarea izolației de pe cablu cu ajutorul stripperului cleștelui de sertizat pe o distanță de 1-1,5 cm. Se aranjează firele conform ordinii dorite (conexiune directă sau cross) și se scurtează la o distanță de circa 1 cm de izolație. Capătul astfel rezultat se introduce în mufa RJ45 cu precizarea că izolația trebuie să pătrundă și ea în interiorul conectorului, cît să poată fi prinsă de clema din plastic a acestuia. Se evită, astfel, tensionarea și detorsadarea firelor în timpul manipulării cablului.

Cu ajutorul cleștelui de sertizat se fixează firele în conector. În final se recomandă verificarea cablului cu ajutorul unui tester, deoarece, așa cum veți vedea în paragraful următor, semnalele electrice pot fi influențate.

Vom încheia acest subiect cu cîteva reguli ce trebuie respectate atunci cînd faceți instalări de cabluri :

- toate componentele trebuie să fie de categoria 5e pentru a se atinge performanțele corespunzătoare ;
- cablurile trebuie instalate fără a avea deformații sau noduri ;
- cablurile nu trebuie trase pe lîngă colțuri care formează unghiuri drepte ;
- la instalările verticale este preferabil să se dea drumul cablului, și nu să fie tras, pentru a se evita tensiunile ;
- folosiți pe cît posibil cabluri de la producători certificați în acest sens.

8.3. Factori care afectează semnalele dintr-o rețea[1]

În cadrul sistemelor electronice, informațiile sînt reprezentate cu ajutorul unei cifre binare : 0 sau 1. Concret, într-un mediu de transmisie bazat pe cupru, cifra 0 este reprezentată prin 0 volți, în timp ce cifra 1 este reprezentată prin 5 volți. Prin urmare, bitul de care tot se vorbește este un puls electric de 0 sau 5 volți !

În cazul semnalelor optice, lucrurile nu diferă prea mult : bitul 0 este codat prin absența luminii sau o lumină cu intensitate scăzută, în timp ce bitul 1 este codat prin prezența luminii.

Nu de puține ori, rețelele sînt proiectate fără a exista cerințe legate de performanța acestora. Și asta nu din vina proiectanților, ci a clienților care dezvoltă sistemele fără a respecta o metodologie anume.

Propagarea

Funcționarea corectă a mecanismului prin care se realizează controlul accesului la mediu impune ca toate interfețele Ethernet să răspundă la semnalele recepționate într-o perioadă de timp dată.

Propagarea se referă la biții (reprezentați prin energie electrică) ce traversează un mediu de transmisie. Viteza cu care aceștia se propagă depinde de materialul din care este realizat respectivul mediu, geometria cablajului și structura acestuia, precum și de frecvența pulsului electric al dispozitivelor prin care tranzitează semnalul.

Timpul necesar unui bit să traverseze de la un capăt la altul și înapoi mediul se numește *Round Trip Time* (*RTT*), sau *timp de întoarcere*. Timpul de întoarcere maxim este strict limitat pentru a asigura că fiecare interfață de rețea poate recepționa toate semnalele din linia de comunicație într-o perioadă de timp specificată. Cu cît este mai lung un segment de rețea, cu atît mai mult timp îi ia unui semnal să îl parcurgă.

Funcționarea corectă a unei rețele Ethernet depinde de mediul de transmisie folosit în cadrul segmentelor și de respectarea regulilor de proiectare.

RTT-ul este o primă măsurătoare ce se poate efectua cu privire la întîrzierile care pot să apară la un moment dat.

1. Vezi și http://www.cabletesting.com/CableTesting.

```
C:\>ping 193.226.23.4

Pinging 193.226.23.4 with 32 bytes of data:

Reply from 193.226.23.4: bytes=32 time=4ms TTL=62
Reply from 193.226.23.4: bytes=32 time=3ms TTL=62
Reply from 193.226.23.4: bytes=32 time=1ms TTL=62
Reply from 193.226.23.4: bytes=32 time=1ms TTL=62

Ping statistics for 193.226.23.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 4ms, Average = 2ms

C:\>_
```

Figura 8.3.1. Fereastra de răspuns la comanda ping

Timpul de propagare nu reprezintă o problemă, ci o situaţie pe care trebuie să fiţi siguri că o puteţi stăpîni. Dacă este prea mare, trebuie să reevaluaţi modul în care reţeaua va face faţă întîrzierilor care apar în transmisia datelor. Dacă, în schimb, acest timp este prea scurt, trebuie să ştiţi cum să-i „frînaţi", sau să-i salvaţi temporar (*buffering*) astfel încît celelalte echipamente din reţea să aibă acces la ei.

Într-o reţea Ethernet cu o lăţime de bandă de 10 Mbps, timpul necesar transmiterii unui bit[1] este de 100 nanosecunde. În continuare, vă prezentăm valorile întîrzierilor pe un segment, valori ce pot fi folosite la calcularea întîrzierii totale (valori exprimate în *bit time*):

Tipul segmentului	Lungimea maximă a segmentului (în metri)	Întîrzierea (RTT)
10BASE5	500	0.0866
10BASE2	185	0.1026
10BASE-T	100	0.113
10BASE-FL	2000	0.1

În calcularea întîrzierii totale a unei reţele se porneşte de la întîrzierea cea mai mare identificată pe fiecare segment de reţea (sau cea mai mare întîrziere care poate să apară pe fiecare segment). Prin însumarea respectivelor valori ale RTT se obţine valoarea totală a întîrzierii din reţea. Standardele recomandă ca la această valoare să se adauge o marjă de 5 bit time. Dacă rezultatul este egal sau mai mic de 512 bit time (adică 51.2 microsecunde), ruta respectivă este considerată bună. Acest lucru înseamnă că ultima staţie situată pe cel mai slab segment din această reţea primeşte notificări cu privire la apariţia coliziunilor într-un interval maxim de 57512 bit time: 511 biţi ai cadrului plus 64 din preambul şi delimitatorul de start. Dacă lucrurile merg bine cu cel mai slab segment de reţea, ar trebui să nu existe probleme cu celelalte.

Lucrurile nu se termină aici, pentru că există o situaţie aparte care trebuie luată în calcul: ruta pentru care se realizează calculele să aibă la extremităţi segmente de alt tip decît restul reţelei.

1. *Bit time* - numărul de biţi transportaţi între dispozitivele din reţea într-o perioadă de timp dată (de obicei, o secundă).

Dacă valoarea întîrzierii nu este specificată de producătorul cablului respectiv, trebuie calculată. Timpul de propagare este specificat de producători ca procent din viteza de propagare a luminii[1].

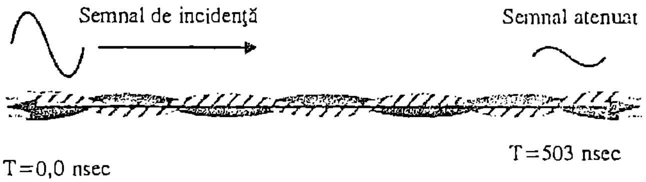


Figura 8.3.2. Întîrzierea pe cablu

Întîrzierea normală la propagare pentru un cablu UTP categoria 5 este 5 nanosecunde pe metru, iar cea maximă admisă este de 5,7 ns/metru. Pentru un segment cu o lungime de 100 metri, întîrzierea poate fi cea din figura de mai sus.

Atenuarea

Atenuarea este cuvîntul prin care se descrie pierderea de energie în timpul propagării semnalului printr-un mediu de transmisie. Aceasta înseamnă că un bit îşi pierde din voltaj sau din amplitudine, pe măsură ce energia este transferată de la calculator către cablul prin care circulă. Pierderea se exprimă în decibeli pe kilometru, iar energia pierdută depinde de frecvenţa semnalului.

Dacă se aleg cu grijă mediile de transmisie, dacă se poziţionează corect, atenuarea electrică poate fi redusă. Nu poate fi însă eliminată, pentru că nu poate fi eliminată rezistenţa materialelor. Atenuarea apare şi în cazul fibrei optice care absoarbe şi distruge o parte din pulsul de lumină, pe măsură ce acesta o traversează. Acest lucru poate fi redus prin alegerea unei lungimi de undă corespunzătoare, a culorii etc.

Reţineţi însă că, deocamdată, pierderea de semnal din mediile de transmisie este inevitabilă. Ea apare şi în cazul undelor radio sau al microundelor care sînt absorbite de moleculele specifice atmosferei.

Atenuarea poate afecta reţeaua dacă nu sînt impuse unele limitări în ceea ce priveşte cablul prin care sînt transmise semnalele. Dacă un cablu este prea lung, un bit care la sursă este 1, poate să ajungă la destinaţie ca 0. Efectele atenuării pot fi reduse prin folosirea unor medii de transmisie de calitate superioară, prin structurarea reţelei şi instalarea de repetoare.

Cel mai adesea, atenuarea este influenţată de lungimea mediului de transmisie şi de frecvenţa semnalului.

1. *Nominal Velocity of Propagation*. Un cablu cu NVP de 75 transmite semnalul cu o viteză egală cu 75% din viteza luminii. Majoritatea cablurilor au NVP cuprinsă în intervalul 0,6 – 0,9c (c = viteza luminii).

Reflecţia

Reflecţia apare în semnalele electrice, cînd din cauza discontinuităţii pe care biţii o întîlnesc în cablu, o parte din energia electrică se reflectă. Dacă nu este controlată în mod corespunzător, această energie poate induce confuzie printre ceilalţi biţi care traversează linia. În funcţie de cablul şi conexiunea folosite, reflecţia poate fi o problemă sau nu.

În cazul semnalelor optice, acestea se reflectă indiferent dacă sticla prezintă discontinuităţi sau nu. Aduceţi-vă aminte că noaptea, cînd priviţi pe fereastră, vă vedeţi propria reflecţie. Acest fenomen apare şi în cazul undelor radio şi al microundelor atunci cînd acestea circulă prin atmosferă.

Pentru ca reţeaua să ajungă la performanţe optime, este important ca mediul de transmisie să aibă o anumită impedanţă care să răspundă cerinţelor componentelor electrice de la nivelul NIC. În caz contrar, se poate ajunge la interferenţe de semnale, biţii transmişi ajungînd să fie confuzi.

Zgomotul

În sistemele de comunicaţii, interferenţele statice care distrug integritatea unui semnal ce traversează acea linie sînt referite ca zgomote. Cu alte cuvinte, este vorba de modificarea voltajului, a semnalului optic sau a undei electromagnetice ca urmare a captării de energie din alte surse. Nu există semnal electric care să nu aibă „zgomote" : fiecare bit care traversează liniile de transmisie recepţionează semnale de la diferite surse.

Cînd zgomotul dintr-un cablu are la origine semnalele care traversează alte fire, se spune că avem de a face cu o încrucişare (*crosstalk*). Dacă două fire aflate în apropiere unul de altul nu sînt corect ecranate, energia dintr-un fir poate fi transferată celuilalt şi viceversa (gîndiţi-vă la principiul de funcţionare a antenelor).

Zgomotele datorate liniilor de tensiune reprezintă o altă problemă crucială a reţelelor. Vrem, nu vrem, în interiorul clădirilor, pereţii sînt traversaţi de liniile de tensiune. Dacă nu sînt izolate corespunzător, acestea pot afecta traficul reţelei. Poate sînteţi surprinşi dacă aflaţi că pînă şi „zgomotul" datorat tensiunii dintr-un monitor sau hard disk poate provoca efecte negative! Toate aceste efecte negative pot fi combătute cu ajutorul „împămîntării".

Interferenţele care pot să apară între doi conductori sînt destul de greu de identificat, cu atît mai mult cu cît firele acţionează, de cele mai multe ori, ca nişte antene pentru „zgometele" electrice (dacă nu sînt torsadate). Calculatorul trebuie să poată să discearnă între semnalele digitale şi impulsurile electrice ce interferează cu acestea.

Alte surse externe ale semnalelor electrice ce pot afecta calitatea acestor semnale sînt: motoarele electrice, sistemele radio şi chiar lumina. În limbajul „reţelistic" acestea sînt denumite *interferenţe electromagnetice* şi *interferenţe radio*.

Spuneam că fiecare cablu în parte poate acţiona ca o antenă. Dacă ne referim la UTP, sînt opt fire care se pot manifesta astfel. Ce se întîmplă de fapt? Fiecare fir din cablu absoarbe semnalele electrice din celelalte fire ale cablului şi din sursele externe ale acestuia. Dacă „zgomotul" astfel rezultat este destul de ridicat, cartela de reţea nu va mai şti să facă diferenţă între acest zgomot şi semnalele care reprezintă date.

Problema interferenţelor este deosebit de importantă dacă ţinem cont de faptul că majoritatea LAN-urilor folosesc frecvenţe cuprinse între 1-100 megahertzi, bandă în care operează multe dintre posturile de radio FM sau semnalele TV.

Ideal ar fi ca înainte de proiectarea clădirii să se poarte discuții cu cel care va realiza instalația electrică, pentru a ști cu exactitate pe unde vor fi trase firele de alimentare cu electricitate. Se va încerca, astfel, ca liniile de comunicație ale rețelei să nu fie în apropierea (să nu se intersecteze) liniilor electrice. Pentru a evita neajunsurile create de acest tip de emisii, proiectanții de materiale pentru rețea folosesc două tehnici : protejarea/izolarea și anularea.

Protejarea presupune că fiecare pereche de fire sau grup de perechi este izolată de celelalte printr-un înveliș izolant. Acesta acționează ca o barieră împotriva oricăror interferențe. Dar aceasta nu este o soluție tocmai viabilă, deoarece înfășurarea unui material protector pe fiecare pereche de fire duce, pe de o parte, la creșterea diametrului cablului, iar pe de altă parte, la creștere costului de producție a acestuia.

Prin urmare, astăzi, cea mai folosită tehnică de protecție împotriva interferențelor o reprezintă anularea. Circulația curentului electric prin fire creează un cîmp magnetic circular în jurul acestora. Direcția forțelor acestui cîmp este dată de direcția de circulație a curentului electric prin respectivul fir. Dacă două fire fac parte din același circuit, electronii se deplasează de la polul negativ sursă, prin fir, către destinație. Apoi, de la destinație se întorc către polul pozitiv sursă. Aflîndu-se în apropiere, cîmpurile magnetice ale celor două fire se vor anula reciproc și vor reuși să anuleze și orice alt cîmp magnetic din exteriorul circuitului din care fac parte. Înfășurarea firelor între ele (torsadarea) poate crește efectul anulării (*http : //epics.aps.anl.gov/techpub/lsnotes/ls232/ls232.htm*).

La trecerea curentului printr-un fir se creează un cîmp electromagnetic care poate să interfereze cu cel creat în firele adiacente. În cazul cablului UTP, fiecare pereche de fire este torsadată pentru a se anula cîmpurile electromagnetice create în cele două fire. Cu cît sînt mai des torsadate firele, cu atît mai mult crește efectul anulării și rata reală de transfer a datelor prin respectivul cablu. Dacă firele nu sînt corect torsadate, efectul este apariția NEXT (*near-end crostalk* – încrucișare[1] măsurată la plecare).

Fenomenul este similar cu ce se întîmplă în cazul telefoniei cînd se ating două fire și se aud simultan două convorbiri. În cazul rețelelor, fenomenul apare în momentul în care semnalul mai puternic dintr-o pereche de fire este recepționat de o pereche adiacentă de fire. NEXT reprezintă acea porțiune a semnalului transmis care se cuplează electromagnetic cu semnalul recepționat.

Simplificat, lucrurile se prezintă astfel :

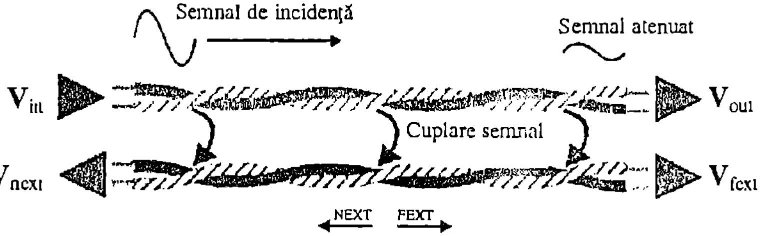


Figura 8.3.3. Zgomotul pe cablu

1. Termenul exact este *diafonie*.

FEXT (*far end crosstalk* – încrucișare măsurată la sosire) este similară cu NEXT, diferența constînd în faptul că încrucișarea este măsurată la capătul cel mai îndepărtat față de punctul de generare.

Am insistat ceva mai mult asupra acestui subiect, deoarece este bine de știut că folosirea cablurilor din categoria 5, a prizelor și conectorilor de calitate nu conduce în mod automat la obținerea performanțelor unei rețele din această categorie.

Latența

În cadrul unei rețele, latența este de multe ori sinonimă întîrzierii : timpul necesar unui pachet să ajungă de la sursă la destinație. În practică, acest fenomen are mai multe surse.

Putem vorbi, în primul rînd, despre *dispersia* caracteristică materialului din care este realizat un cablu. Este posibil ca 1 bit să interfereze atît cu precedentul, cît și cu următorul. Iar cînd se transmit milioane de biți, este posibil ca acest lucru să depășească limitele normale în ceea ce privește timpul de transmisie.

Toate sistemele digitale au un ceas (sau o frecvență de tact la care lucrează), ceea ce înseamnă că pulsurile acestui ceas conduc la apariția unui eveniment sau altul : CPU să realizeze un anumit calcul, datele să fie scrise în memoria calculatorului, cartela de rețea să transmită mai departe biții pe care i-a recepționat... Dacă ceasul unei surse care transmite date nu este sincronizat cu cel al destinatarului, se poate ajunge la distorsionarea în timp a transmisiei, ceea ce face ca biții să ajungă la destinație mai tîrziu decît ar fi normal.

Latența, cunoscută și sub denumirea de întîrziere, are două cauze principale. Prima se datorează teoriei relativității. Prin firele metalice și prin fibra optică, semnalele se propagă cu o viteză mai mică decît a reţelei ($2,3*10^8$ m/s, respectiv $2*10^8$ m/s). Prin urmare, pentru a traversa o anumită distanță, biții au nevoie de un anumit timp. La aceasta se mai adaugă și faptul că majoritatea componentelor electronice ale calculatorului induc latență (este vorba despre fracțiuni de secundă !)

Dispersia poate fi „combătută" prin proiectarea corespunzătoare a cablurilor, reducerea lungimii acestora și folosirea impedanței corespunzătoare. În cazul fibrei optice, limitarea dispersiei presupune folosirea unei lumini laser cu o lungime de undă specifică.

În cazul distorsiunii, lucrurile sînt ceva mai complicate deoarece este vorba de sincronizări complexe la nivel hardware.

Latența se reduce cu ajutorul echipamentelor de rețea și a protocoalelor specifice nivelurilor modelului OSI.

8.4. 10BaseT (Ethernet)

Pentru că tot sînt la modă „rețelele de cartier", continuăm cu un exemplu pentru astfel de cazuri.

Din punctul de vedere al topologiei și cablurilor folosite, rețelele Ethernet 10BaseT folosesc ca mediu de transmisie UTP cat3 (sau mai bun) într-o topologie stea. Fiecare nod din rețea are propria sa legătură la un repetor (*hub*), legătură care nu poate depăși 100 de metri.

Se poate folosi și o topologie tip arbore, în care un repetor central este conectat la alte repetoare. Nu este exclusă nici posibilitatea combinării tehnologiilor (10Base-T cu 10Base-2, pentru a reveni la exemplu) :

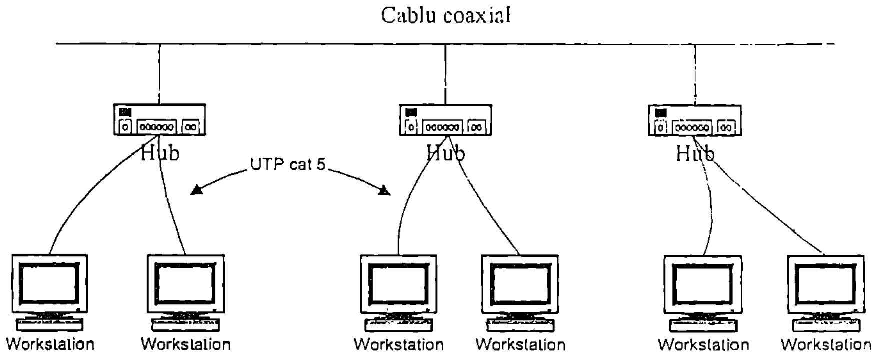


Figura 8.4.1. O rețea 10BaseT

În această situație, nu uitați de regula numărului maxim de repetoare pe un segment.

Și acum se pune întrebarea de bază : cînd se pretează o astfel de rețea ? Avantajele o recomandă pentru anumite aplicații, dar, în același timp, sînt situații cînd este bine să fie evitată.

Atît timp cît fiecare nod dintr-o astfel de rețea are propria sa conexiune, este eliminată probabilitatea ca defectarea sa să provoace întreruperi în întregul sistem. Mai mult, repetoarele au implementată o funcție de „partiționare" prin care detectează eventualele probleme apărute la nivelul porturilor și deconectează respectivul nod. Efectul unei astfel de facilități constă în ușurința cu care poate fi depanată o astfel de rețea.

Deconectarea unui nod sau adăugarea unuia nou nu pune probleme pentru ceilalți membri ai rețelei.

Problema cea mai spinoasă legată de 10Base-T ține de lungimea maximă a segmentului, limitare care trebuie depășită prin folosirea altor tehnologii.

8.5. 100 BaseTX (Fast Ethernet)

Mediile de transmisie folosite în rețelele Fast Ethernet depind de varianta care se dorește a fi dezvoltată :

- 100 Base-TX folosește cablul UTP cat5 ;
- 100 Base-T4 folosește patru perechi de UTP cat3 ;
- 100 Base FX folosește fibra optică multimod.

Dacă ne întoarcem cîteva pagini la subiectul legat de întîrzierea indusă de mediile de transmisie, în cazul rețelelor Fast Ethernet, aceasta reprezintă aproximativ 10% din ceea ce se întîmplă în rețelele cu lățime de bandă de 10 Mbps !

Prin urmare, proiectarea unei rețele Fast Ethernet pornește de la calcularea vitezei de propagare a semnalului. Pentru aceasta trebuie identificate două stații ale viitoarei rețele aflate la distanța maximă și unde va fi localizat repetorul între aceste stații. Dacă se respectă toate specificațiile tehnice și întîrzierea nu este mai mare de 512 bit time pe un segment, atunci totul este în regulă. În caz contrar, rețeaua trebuie segmentată (folosim un switch).

După cum se vede din fig. 8.5.1, avem o rețea 100 BaseTx între două PC-uri conectate la un hub. Cablurile prin care se conectează cele două PC-uri au lungimea maximă admisă de standarde.

Pentru cele două segmente de cablu întîrzierea totală va fi 222,4 bit time (111,2 + 111,2 conform tabelului de mai jos). La aceasta se adaugă întîrzierea indusă de repetor, care este 92, și cea a plăcilor de rețea ale celor două PC-uri, care este 100. În total, rezultă o întîrziere de 414.4 bit time. După cum observați, valoarea este mai mică decît 512, ceea ce înseamnă că rețeaua noastră este bună din acest punct de vedere.

Iată și cîteva valori ale întîrzierii induse de fiecare tehnologie folosită în cadrul Fast Ethernet:

Întîrzierea dus-întors la propagare (RTT) în bit time[1]		
Echipament	Întîrziere/metru	Întîrzierea totală
2 NIC TX-FX	-	100
Segment cablu UTP Cat 5	1,112	111,2 (100 Metri)
Segment fibră optică	1,00	412 (412 Metri)
Repetor Clasa I	-	140
Repetor Clasa II (toate porturile sînt TX/FX)	-	92
Convertor 100 Base-TX la 100 Base-FX	-	50 - 100

Așa stau lucrurile în teorie. Să ne apropiem însă ceva mai mult de realitate (vezi fig. 8.5.2).

De unde pornim? Trebuie să identificăm cea mai lungă cale între două calculatoare. După cum se vede și din schemă, este vorba de PC1 și PC3 între care distanța este de 185 metri. Echipamentele cu care ne întîlnim pe acest traseu sînt:

- două plăci de rețea 100TX (100 bit time);
- două repetoare clasa II (2*92 = 184 bit time);
- 80 metri cablu de la PC1 la repetor (80*1,112 = 88,96 bit time);
- 5 metri cablu între repetoare (5*1,112 = 5,56);
- 100 metri cablu de la PC3 la repetor (100*1,112 = 111,2 bit time).

1. Conform IEEE 802.3u-1995, „Media Access Control (MAC) Parameters, Physical Layer, Medium Attachment Units and Repeater for 100 Mb/s Operation, Type 100BASE-T".

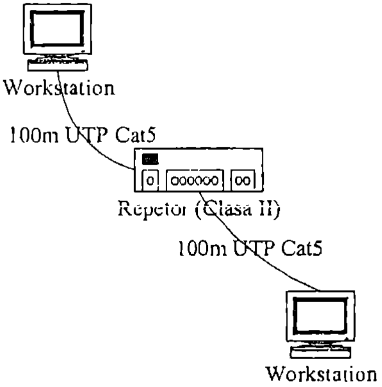


Figura 8.5.1. Latența pentru o rețea Fast Ethernet

Întîrzierea totală va fi 489,72 bit time, ceea ce înseamnă că rețeua este în regulă. Dacă însă vom fi nevoiți să mai adăugăm un repetor (adică o întîrziere suplimentară de 92 bit time), vom depăși valoarea de 512 bit time!

Cum se rezolvă o astfel de problemă? O soluție o reprezintă repetoarele *stackable* (modulare). Acestea sînt hub-uri conectate între ele prin porturi speciale (*stack*). Toate hub-urile dintr-o astfel de stivă formează o singură unitate logică.

Cea de a doua soluție se referă la folosirea switch-urilor sau a fibrei optice, dacă trebuie conectate dispozitive aflate la o distanță mai mare de 100 metri.

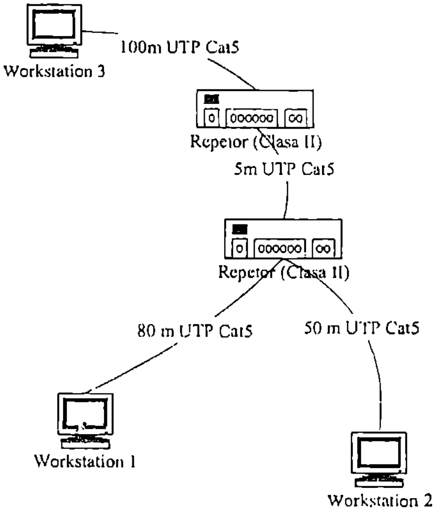


Figura 8.5.2. Exemplu de rețea pentru calcularea latenței

CAPITOLUL 9

Comutarea pachetelor în rețelele de calculatoare

Switching-ul (comutarea pachetelor) reprezintă o tehnologie ce contribuie la diminuarea congestiei în rețelele Ethernet, Token Ring și FDDI prin reducerea traficului și creșterea disponibilității lățimii de bandă. Astăzi, switch-urile au ajuns să înlocuiască tot mai mult hub-urile, deoarece sînt proiectate să funcționeze în infrastructura existentă deja în rețea, fără a perturba traficul acesteia.

9.1. Funcțiile unui switch

Switch-urile au ajuns astăzi să fie considerate componenta fundamentală prin care se realizează segmentarea celor mai multe rețele[1]. Ele permit utilizatorilor dintr-o rețea să transmită informații, prin același mediu, în același timp, fără a încetini traficul. Așa cum routerele permit diferitelor rețele să comunice unele cu altele, switch-urile permit diferitelor noduri (nod = un punct de conexiune dintr-o rețea, de obicei un calculator) din rețea să comunice direct unele cu altele, într-o manieră eficientă.

Prin porturile sale, un switch împarte rețeaua în mai multe canale de comunicație. Aceste canale independente cresc randamentul switch-ului în ceea ce privește lățimea de bandă folosită. Switch-urile mai simple sînt autoconfigurabile, prin urmare, nu este nevoie de personal specializat pentru punerea lor în funcțiune.

În cuvinte simple, modul de funcționare al unui switch este următorul: pentru un segment de rețea atașat la un port al switch-ului, CSMA/CD va controla accesul la mediul de transmisie pentru respectivul segment. Dacă la respectivul port este atașată o singură stație de lucru, nu este nevoie de nici un mecanism prin care să se controleze accesul la mediu. Switch-ul verifică adresele MAC sursă și destinație ale cadrelor pe care le recepționează și transmite respectivele cadre către porturile corespunzătorare.

Prin urmare, comutarea pachetelor la nivelul 2 OSI se bazează pe hardware sau, altfel spus, folosește adrese fizice (MAC).

1. http://www.cisco.com/warp/public/473/lan-switch-cisco.shtml.

Un switch îndeplinește două funcții principale:

- *Comutarea cadrelor*. Această funcție are loc atunci cînd un cadru ajunge la switch dintr-un anumit mediu sau de pe un anumit port și este transferat către un alt mediu/port.
- *Gestionarea operațiilor de comutare*. Switch-ul creează și întreține tabele de comutare sau de filtrare folosind ASIC - Application Specific Integrated Circuits.

Fiecare switch folosit într-o rețea Ethernet induce latență. Un switch interpus între un server și o stație de lucru crește timpul de transmisie cu 21 microsecunde. Un pachet de 1000 bytes are un timp de transmisie de 800 microsecunde. Dacă comutarea realizată de switch este de tip *store-and-foreward*, latența indusă crește.

Tot la capitolul generalități menționăm cele două tipuri de switching: de nivel 2 sau de nivel 3. Diferența între aceste două tipuri de comutări constă în tipul informațiilor conținute în cadru: la nivel 2 se folosește adresa MAC, iar la nivel 3 informațiile nivelului 3.

Switch-ul nu analizează informațiile de nivel 3 conținute de un cadru, ci doar adresa MAC a destinatarului. Dacă adresa este cunoscută, cadrul este transmis către interfața/portul corespunzătoare. Switch-ul construiește tabele cu adresele MAC corespunzătoare fiecărui port în parte. Dacă nu se cunoaște adresa destinatarului, cadrul este transmis către toate porturile (broadcast) pentru ca switch-ul să-i poată „învăța" destinația corectă. Cînd este reprimit cadrul, switch-ul adaugă adresa în tabela cu adrese MAC a portului respectiv.

Cu excepția SNA (*Systems Network Architecture*), utilizatorii nu au control asupra adreselor de nivel 2. În majoritatea rețelelor, administratorilor le revine sarcina de a atribui doar adrese de nivel 3. În acest caz, putem spune că administratorii creează rețele locale ce se comportă ca un singur spațiu de adresare (blocul-strada-orașul-țara).

Un switch Ethernet poate „învăța" adresa oricărui dispozitiv din rețea prin citirea adresei sursă conținută în fiecare pachet și notarea portului prin care cadrul a „intrat" în switch. Aceste adrese sînt memorate într-o bază de date. Adresele echipamentelor din rețea sînt memorate în mod dinamic, altfel spus, pe măsură ce apare un dispozitiv nou, adresa sa este citită, învățată și memorată într-o zonă de memorie (CAM - *content addressable memory*). Cînd switch-ul identifică o adresă pe care nu o regăsește în CAM, o memorează pentru o utilizare viitoare. În momentul memorării, adresa este „ștampilată" și cu data cînd a fost adăugată în CAM. Ori de cîte ori o adresă este referită sau adăugată în CAM, i se înregistrează și noua dată (inclusiv ora) la care a avut loc operațiunea. Adresele la care nu se face referire o anumită perioadă de timp sînt șterse din CAM. Prin acest mecanism, baza de date cu adresele MAC ale dispozitivelor din rețea este actualizată în mod constant.

9.2. Funcționarea switch-ului

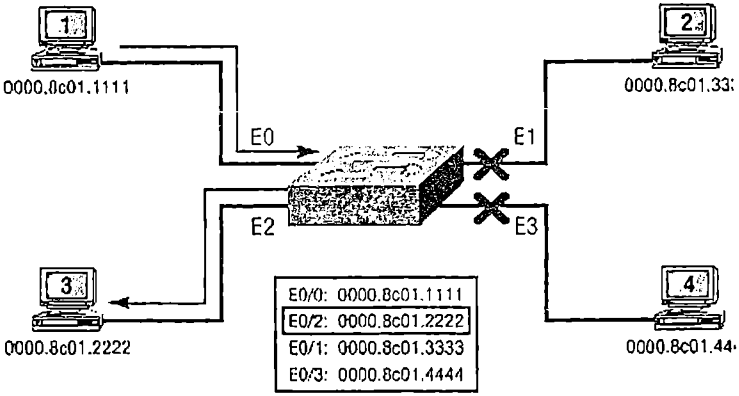


Figura 9.2.1. Funcționarea unui switch
(Sursa http : //www.cisco.com/warp/public/473/lan-switch-cisco.shtml)

Pornind de la imaginea de mai sus, vom încerca să vedem mai în detaliu cum funcționează un switch. La pornire, tabela cu adrese MAC nu conține nici o înregistrare. Cînd un calculator (1) transmite și un port recepționează un cadru, switch-ul preia adresa MAC a calculatorului sursă și o plasează în tabela de filtrare împreună cu portul de unde a fost preluat. Avînd în vedere că destinatarul nu este cunoscut, switch-ul nu va avea de ales și va trebui să „inunde" rețeaua cu acest cadru.

Dacă un calculator din rețea (3) răspunde și trimite înapoi un cadru, switch-ul va prelua adresa sursă din acest cadru și o va înregistra în baza de date cu adrese MAC în asociere cu portul de pe care a fost primit. Din acest moment, switch-ul va putea realiza o conexiune punct-la-punct, cadrele fiind transmise doar între cele două calculatoare.

De fiecare dată cînd un cadru este recepționat pe un anumit port, adresa MAC destinație va fi comparată cu înregistrările din baza de date a switch-ului. Dacă această adresă este cunoscută și apare în baza de date, cadrul va fi transmis către portul corespunzător. În caz contrar, cadrul este transmis broadcast (mai puțin portul pe care a fost recepționat), adresa calculatorului care răspunde la broadcast urmînd a fi înregistrată în baza de date cu adrese MAC.

Dacă tot am pomenit de broadcast, trebuie făcută o precizare : cadrele broadcast și multicast nu specifică adrese MAC destinatare. Adresa sursă va fi întotdeauna adresa MAC a dispozitivului care transmite cadrul, în timp ce adresa destinație poate fi o adresă broadcast (toți biții 1) sau una multicast (biții din porțiunea host au valoarea 1). Broadcast-ul va fi transmis către toate rețelele și host-urile acestora, în timp ce multicastul va fi transmis tuturor host-urilor unei anumite rețele.

Ce se întîmplă însă atunci cînd o legătură se întrerupe? Am putea spune că într-o reţea ar fi bine să existe legături redundante. Corect. Această rezolvare însă, mai mult încurcă decît ajută. Atît timp cît broadcast-ul este transmis tuturor reţelelor, furtuna broadcast sau, altfel spus, circulaţia mesajelor în buclă nu poate fi evitată. Ce se întîmplă în astfel de situaţii? Un calculator va primi copii ale aceluiaşi cadru, dar de la surse diferite, de pe segmente de reţea diferite. Tabela cu adrese MAC de pe switch nu mai ştie ce să înregistreze. Switch-ul nu ştie care cadru trebuie transmis în reţea, deoarece tabela MAC este actualizată continuu. Această situaţie are o rezolvare şi se numeşte *Spanning Tree Protocol*.

Comutarea simetrică a pachetelor caracterizează o reţea în care switch-ul alocă lăţimea de bandă în mod egal fiecărui port. Un switch simetric oferă deci conexiuni între porturi cu aceeaşi lăţime de bandă : 10Mbps sau 100Mbps. Spre deosebire de acesta, un switch asimetric oferă conexiuni între porturi cu lăţimi de bandă diferite, cum ar fi o combinaţie 10-100Mbps.

Switch-urile asimetrice sînt folosite mai ales în cazul traficului generat de aplicaţii client-server. Într-un astfel de switch, bufferingul memoriei trebuie să permită traficului de pe portul pe 100Mbps să fie transmis către portul pe 10Mbps, fără să conducă la blocarea acestuia din urmă.

Un switch Ethernet foloseşte o tehnică buffering prin care memorează şi transmite pachetele către porturile corecte. Zona de memorie în care se păstrează datele ce trebuie transmise se numeşte buffer. Această zonă de memorie poate folosi două metode de transmisie a pachetelor : *port-based memory buffering* sau *shared memory buffering*.

În bufferingul de tip port-based, pachetele sînt memorate într-o coadă de aşteptare, în funcţie de portul pe care au „intrat". Un pachet este transmis către destinaţie abia cînd toate pachetele dinaintea sa au fost transmise. Acest lucru face posibil ca un singur pachet să întîrzie întreaga transmisie a pachetelor din memorie, ca urmare a ocupării portului destinaţie (de exemplu.). Această întîrziere apare chiar dacă alte pachete pot fi transmise către porturi care sînt libere.

În bufferingul de tip shared memory, switch-ul depozitează pachetele într-o zonă de memorie care este partajată între toate porturile. Memoria alocată unui port depinde de cît „cere" fiecare port la un moment dat, altfel spus, este alocată în mod dinamic. Pachetele din buffer sînt asociate dinamic portului care transmite. Aceasta oferă posibilitatea ca un pachet să fie recepţionat pe un port şi transmis pe un altul, fără ca datele să mai „stea la coadă".

Switch-ul întreţine o hartă a tuturor porturilor către care trebuie transmis un pachet. După ce transmisia pachetului s-a făcut cu succes, această hartă este ştearsă. Ca efect al memoriei partajate, dimensiunea unui pachet este limitată la dimensiunea bufferului şi nu doar la cea alocată unui anumit port. Ce înseamnă aceasta? Se pot transmite pachete mai mari dacă se distrug cîteva pachete de dimensiuni reduse. Este o facilitate foarte importantă în cazul switch-urilor 10/100Mbps, în care un port pe 100 poate să transmită un pachet către un port pe 10 Mbps.

9.3. Metode de comutare a pachetelor

Latența pachetelor într-un switch depinde, în primul rînd, de modul în care se realizează comutarea acestora. Există trei astfel de metode.

Store-and-forward reprezintă cea mai cunoscută metodă de switching într-o rețea. Înainte de a fi transmis, cadrul este recepționat în totalitate: se citește adresa sursă și/sau destinație și se aplică anumite filtre, se calculează o cifră de verificare a redundanței. În timpul recepționării cadrului apare și latența. Cu cît cadrul este mai mare, cu atît este mai mare și latența indusă ca urmare a timpului necesar citirii sale. Detectarea erorilor mai consumă și ea ceva timp, deoarece switch-ul trebuie să aștepte recepționarea întregului cadru. Dacă există erori, cadrul este distrus. Dacă este prea mic (mai puțin de 64 bytes) sau prea mare (mai mult de 1518 bytes), este de asemenea distrus. Dacă totul este bine, switch-ul caută adresa MAC destinație și determină portul de ieșire.

Cut-through (în timp real) este cea de-a doua metodă de comutare. Înainte de a aștepta recepționarea întregului cadru, switch-ul citește adresa destinație și lansează transmiterea sa. De fapt, switch-ul copie doar adresa destinație (primii 6 bytes de după preambul) în memorie și caută această adresă în tabela sa pentru a determina care este portul de ieșire. Această tehnică reduce latența și, în plus, nici nu detectează erorile așa cum se întîmplă în store-and-forward.

Cut-through are două variante:

- *Fast-forward switching*. Această variantă induce cea mai mică latență, deoarece un pachet este transmis imediat ce a fost identificată adresa destinație. Dezavantajul constă în faptul că sînt transmise mai departe și pachetele ce conțin erori. Chiar dacă aceste situații nu apar în mod constant și NIC-urile renunță la cadrele ce conțin erori, apariția unui trafic inutil în rețea nu este digerată de nici un administrator sîrguincios. Switch-ul măsoară latența pornind de la primul bit recepționat și terminînd cu primul transmis (FIFO).
- *Fragment-free switching*. Această variantă presupune filtrarea și transmiterea numai a fragmentelor de pachete ce nu conțin erori. În mod obișnuit, un fragment ce ia naștere în urma unei coliziuni trebuie să fie mai mic de 64 bytes. Orice pachet mai mare decît această valoare este considerat valid și, prin urmare, este recepționat fără erori. În această situație, switch-ul așteaptă pînă cînd un pachet recepționat este validat și apoi îl transmite către portul destinație.

Latența fiecăruia dintre modurile prezentate depinde de cum se realizează transmisia pachetelor. Cu cît este mai rapid modul de transmitere, cu atît este mai redusă latența. Dar, pentru a se ajunge în această situație, înseamnă că switch-ul alocă mai puțin timp pentru verificarea erorilor. Și, cu cît verificarea erorilor este mai redusă, cu atît mai mult crește numărul retransmisiilor.

9.4. Spanning Tree Protocol (STP)

Principala menire a acestui protocol este de a împiedica apariția așa-ziselor circuite în buclă. STP monitorizează în mod constant rețeaua, izolînd buclele și trecînd anumite conexiuni în stand-by.

Să exemplificăm:

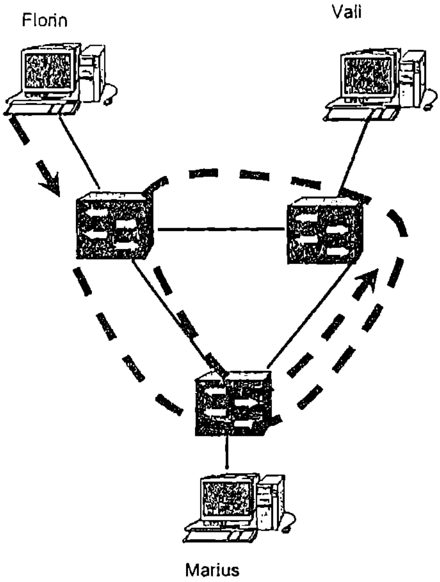


Figura 9.4.1. Comutarea pachetelor fără STP

Figura de mai sus vrea să arate cum circulă un singur cadru trimis de calculatorul lui Florin, dacă STP-ul nu ar fi activat.

Florin trimite un singur cadru unicast către adresa MAC a lui Marius. Calculatorul lui Marius nu este pornit și, prin urmare, switch-ul nu are de unde să îi știe adresa MAC. Acest cadru va circula în rețea la infinit (sau pînă la expirarea timpului de viață) și va fi transmis de către switch către toate porturile active pînă în momentul în care una din legături pică.

În lipsa unui astfel de protocol, o rețea devine inutilizabilă. Algoritmul *spanning tree* atribuie fiecărui port de pe switch mai multe stări:

- *Blocking* – nu se transmite nici un cadru.
- *Listening* – nu se transmite nici un cadru, se „ascultă".
- *Learning* – nu se transmite nici un cadru, se învață adrese.
- *Forwarding* – se transmit cadre, se învață adrese.
- *Disabled* – inactiv.

Revenind la exemplul anterior, cînd Florin va transmite cadre către calculatorul lui Marius, acestea nu vor mai circula în buclă. SW1 va trimite o copie a cadrului transmis de Florin către SW2, dar SW3 nu va putea să transmită această copie către portul 0/27, deoarece acesta este blocat. Pe de altă parte, dacă Vali doreşte să transmită un cadru către Marius, va trebuie să o facă prin intermediul SW1, şi nu direct. Dacă legătura dintre SW1 şi SW3 cade, atunci SW va schimba starea portului 0/27 în *forwarding*.

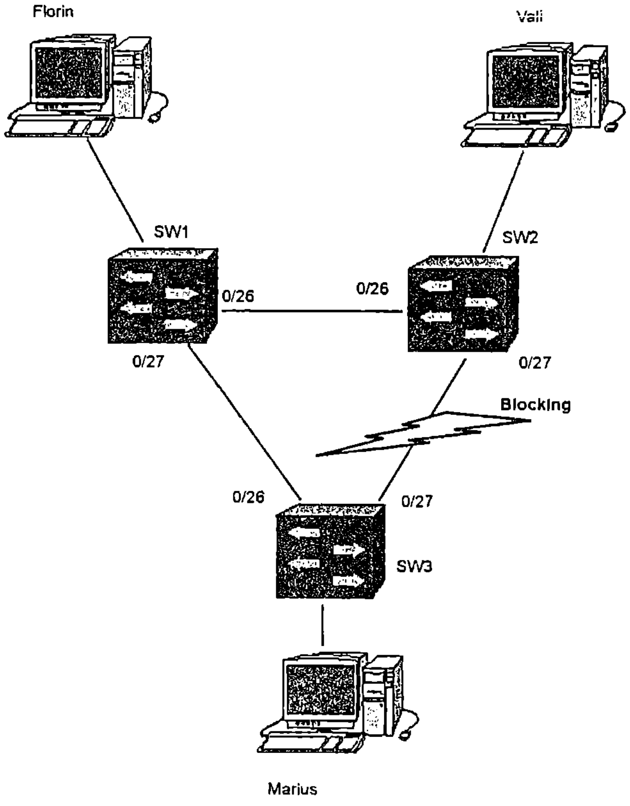


Figura 9.4.2. Spanning Tree Protocol

CAPITOLUL 10

Rețele virtuale

Am văzut că folosirea switch-ului într-o rețea Ethernet are ca efect segmentarea acesteia în domenii de coliziune individuale. Numărul total de segmente ce se pot obține prin folosirea unui switch alcătuiește domeniul de broadcast. Acest lucru înseamnă că toate nodurile aparținînd tuturor segmentelor pot să vadă broadcast-ul transmis de un nod al unui segment.

O rețea virtuală presupune gruparea logică a echipamentelor și/sau utilizatorilor unei rețele fără a mai exista restricții legate de segmentul fizic din care fac parte[1]. Altfel spus, o rețea virtuală reprezintă un domeniu de broadcast dintr-o rețea cu switch-uri.

Cu ajutorul switch-urilor se poate crea o singură rețea virtuală sau mai multe. În cel de al doilea caz, broadcast-ul unei astfel de rețele nu va fi „văzut" de către celelalte. Implementarea rețelelor virtuale permite administratorilor diminuarea domeniilor de broadcast și creșterea disponibilității lățimii de bandă. Și cum în proiectarea unei rețele de multe ori se impune crearea unor astfel de componente, ne-am gîndit să tratăm acest subiect într-un capitol distinct, chiar dacă el ar fi trebuit, în mod firesc, să fie prezentat în capitolul precedent.

10.1. Tipologia VLAN-urilor

Tehnologia pusă la dispoziție de VLAN-uri oferă posibilitatea grupării porturilor și a utilizatorilor în grupuri logice. Dacă această grupare implică folosirea mai multor switch-uri, VLAN-urile pot partaja aceeași clădire, mai multe clădiri sau chiar WAN-uri. Pentru orice arhitectură VLAN, importantă este posibilitatea transferului de informații între switch-uri și routere.

În mod tradițional, routerul gestionează broadcast-ul și procesează rutele pachetelor. Chiar dacă switch-urile unei VLAN preiau o parte din aceste sarcini, routerul rămîne vital pentru arhitectura oricărei rețele, deoarece prin intermediul lui se pot interconecta VLAN-uri diferite.

---

1. Facem precizarea că datorită nenumăratelor soluții și strategii de implementare existente pe piață, este destul de dificil de dat o definiție cît mai exactă a VLAN.

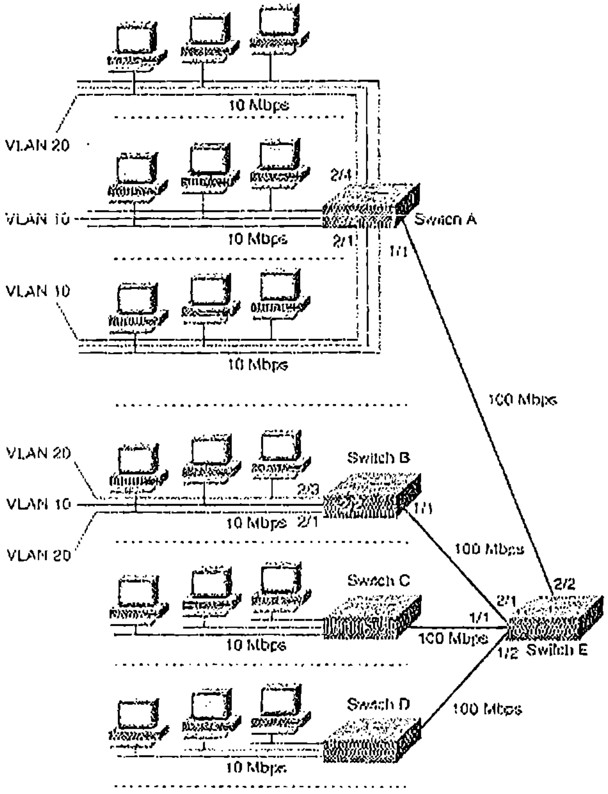


Figura 10.1.1. Exemplu de rețea virtuală
(Sursa : http://www.cisco.com/univercd/cc/td/doc/cisintwk/idg4/nd2023.htm→xtocid3)

Gruparea după porturi

Inițial, multe implementări de VLAN-uri defineau apartenența la un VLAN prin intermediul unei grupări după porturile din switch. În plus, în majoritatea implementărilor inițiale, VLAN-urile erau realizate pentru un singur switch.

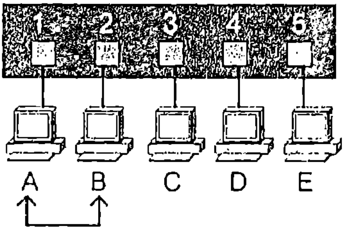


Figura 10.1.2. VLAN cu grupare după porturi

Pentru a doua generaţie de implementări, se poate forma un VLAN prin conectarea mai multor porturi de pe switch-uri diferite.

Gruparea după porturi este cea mai des întîlnită metodă, iar configurarea este destul de uşor de realizat. Definirea VLAN-urilor doar pe baza porturilor nu permite unor VLAN-uri diferite să includă acelaşi segment fizic (sau port de switch). Însă, principala limitare în cazul grupării după porturi este că administratorul reţelei trebuie să reconfigureze VLAN-ul de fiecare dată cînd un utilizator este comutat de pe un port pe altul.

Gruparea după adresa MAC

Apartenenţa la un VLAN se realizează pe baza adresei MAC a staţiei. Switch-ul urmăreşte adresa MAC care aparţine fiecărui VLAN. Cum adresa MAC e o componentă a plăcii de reţea, cînd se schimbă poziţia unei staţii, nu mai este necesară nici o reconfigurare suplimentară pentru ca staţia respectivă să rămînă în acelaşi VLAN.

Gruparea într-un VLAN pe baza adreselor MAC are şi avantaje, şi dezavantaje. Din moment ce adresele MAC sînt la nivelul 2 al modelului OSI şi sînt „arse" în plăcile de reţea, VLAN-urile le permit administratorilor de reţea să schimbe poziţia fizică a unui calculator în reţea, iar acesta să rămînă în continuare în VLAN-ul din care făcea parte, în mod automat. În acest fel, un VLAN definit pe baza adreselor MAC poate fi considerat ca fiind „bazat pe utilizatori".

Unul dintre dezavantajele VLAN-urilor bazate pe adresa MAC e faptul că, iniţial, fiecare staţie trebuie să fie adăugată manual la VLAN, mai precis fiecare adresă MAC de pe placa de reţea. După configurarea manuală iniţială, urmărirea şi repoziţionarea staţiilor (şi implicit a utilizatorilor) sînt automatizate, acest lucru fiind specific fiecărui echipament, în funcţie de producătorul său. Acest dezavantaj al unei configurări manuale iniţiale este cu adevărat problematic în cazul în care, în faza iniţială, e necesară repartizarea la VLAN-uri a unui număr foarte mare de utilizatori, de ordinul miilor, în reţelele foarte mari. Unii producători au venit cu soluţii automatizate intermediare, prin care diferite instrumente software creează VLAN-uri, pe baza adreselor MAC, la nivel de subreţea.

VLAN-urile bazate pe adresele MAC ale staţiilor, implementate în medii distribuite, vor întîmpina probleme mari în ceea ce priveşte performanţa reţelei, pentru că traficul dinspre şi spre staţii din VLAN-uri diferite va trece prin aceleaşi porturi. În plus, metoda primară de comunicare a informaţiilor de apartenenţă la un VLAN bazat pe adrese MAC va avea ca efect scăderea performanţelor pentru implementări la scară mare.

O altă limitare a grupării într-un VLAN pe baza adreselor MAC e atunci cînd un utilizator foloseşte un notebook şi pentru a se putea conecta la reţea, conectează notebook-ul său la aşa-numitele staţii de andocare (*docking stations*). Notebook-urile bineînţeles că au o adresă MAC care rămîne aceeaşi, indiferent de locaţia utilizatorului. Staţiile de andocare au şi ele o adresă MAC unică, dar cum utilizatorul îşi modifică mereu poziţia, adresele MAC ale staţiilor de andocare vor fi mereu altele. Adresa MAC variind mereu, va fi imposibilă şi rămînerea utilizatorului mereu în acelaşi VLAN.

VLAN-urile bazate pe nivelul 3 OSI

VLAN-urile bazate pe informaţiile de la nivelul 3 al modelului OSI folosesc tipul protocolului (în cazul în care suportă mai multe tipuri de protocoale) sau adresele de la

nivelul rețea (adresa de subrețea pentru rețelele TCP/IP) pentru a putea determina apartenența la un anumit VLAN. Deși aceste VLAN-uri lucrează cu informații de la nivelul 3, aceasta nu e o funcție de rutare și nu trebuie confundată cu rutarea la nivelul rețea. Deși un switch analizează adresa IP a pachetului pentru a determina apartenența la un VLAN, nu se calculează nici o rută a pachetului. Noile switch-uri însă știu să interpreteze și informațiile încapsulate de protocoalele RIP sau OSPF. Cadrele ce traversează un switch sînt trimise pe un port sau altul pe baza algoritmului *Spanning Tree*. Astfel, din perspectiva unui switch ce e folosit într-un VLAN bazat pe nivelul 3 OSI, acesta e văzut ca o rețea plată, ca topologie, fără nici o ierarhie, ca și cînd ar lucra numai la nivelul legătură-date.

O dată făcută diferența între VLAN-urile bazate pe informații de la nivelul rețea și rutare, trebuie menționat că anumiți producători au dotat swhitch-urile pe care le realizează cu capacități de procesare a informațiilor de nivel 3. Aceste capacități au dus la manifestarea unor funcții ce sînt asociate în mod obișnuit cu rutarea. Mai mult, switch-urile „multi layer" au funcții de forwarding ale pachetelor datorită chip-set-urilor ASIC încorporate. Însă, indiferent unde ar fi localizate switch-urile sau routerele într-un VLAN, rutarea este necesară pentru a asigura conectivitatea între VLAN-uri distincte.

Există cîteva avantaje evidente în definirea VLAN-urilor la nivelul 3 OSI. În primul rînd, ele asigură partiționarea pe baza tipului de protocol. Aceasta se poate dovedi o opțiune atractivă pentru administratorii de rețea, care trebuie să implementeze o strategie de VLAN pe baza unui serviciu sau a unei aplicații. În al doilea rînd, utilizatorii își pot modifica locația fizică fără a mai fi nevoie să reconfigureze adresa de rețea a stației lor (acesta este un avantaj în special pentru cei ale căror stații sînt configurate pe TCP/IP). În al treilea rînd, definirea VLAN-urilor la nivelul 3 poate elimina nevoia pentru „frame tagging", necesară pentru a comunica între switch-uri informații referitoare la apartenența la un VLAN. Se reduce astfel traficul general.

Unul dintre dezavantajele definirii VLAN-urilor la nivelul 3 al modelului OSI (în comparație cu definirea pe baza adreselor MAC, sau pe baza porturilor) este performanța. Analiza adreselor de la nivelul rețea în pachete este o acțiune care necesită mai mult timp decît analiza adreselor MAC din frame-uri. Din acest motiv, switch-urile care folosesc informații de la nivelul rețea pentru definirea VLAN-urilor au o latență mai mare decît cele care folosesc informații de la nivelul legătură-date. Această diferențiere se întîlnește la majoritatea producătorilor de switch-uri, însă nu este o regulă general valabilă.

VLAN-urile definite la nivelul rețea sînt eficiente în rețele bazate pe protocoalele TCP/IP, dar sînt mai puțin eficiente pentru rețelele bazate pe protocoalele IPX, DECnet sau AppleTalk, care nu presupun configurarea manuală la desktop. În plus, VLAN-urile definite la nivelul rețea al modelului OSI întîmpină dificultăți la procesarea pachetelor unor protocoale nerutabile, precum NetBIOS. Stațiile finale care rulează protocoale nerutabile nu pot fi diferențiate între ele, astfel că nu pot fi definite ca și părți componente ale unui VLAN configurat la nivelul rețea.

10.2. Configurarea VLAN-urilor

Manual

Configurarea VLAN-ului se face doar manual. Atît setarea inițială, cît și modificările și repoziționările ulterioare de echipamente în rețea sînt controlate de către administratorul de rețea. Configurarea manuală are însă și avantajul controlului total asupra rețelei. Însă, cu cît complexitatea rețelei și dimensiunea acesteia crește, cu atît devine mai dificilă întreținerea acesteia, astfel încît mentenanța manuală este aproape imposibilă.

În plus, administrarea manuală înlătură însăși unul dintre avantajele pe care le presupune existența unui VLAN, și anume eliminarea timpului necesar pentru administrarea schimbărilor și mutărilor (deși mutarea unui utilizator în interiorul unui VLAN este mai ușor de realizat decît mutarea unui utilizator dintr-o subrețea în alta).

Semi-Automat

Configurarea semi-automată se referă la existența posibilității de a automatiza fie configurarea inițială, fie modificările și mutările ulterioare, fie ambele. Automatizarea inițială e realizată de obicei printr-un set de instrumente care mapează VLAN-urile la subrețelele existente. Configurarea semi-automată poate de asemenea însemna că inițial, configurarea se realizează manual, urmînd ca toate modificările și mutările ulterioare să fie îndeplinite automat. Combinarea configurării inițiale automate cu urmărirea automatizată a schimbărilor tot presupune configurare semi-automată, pentru că administratorul are încă, în orice moment, posibilitatea de a interveni manual și de a face orice schimbare.

Automat

Un sistem care are automatizată funcția de configurare a unui VLAN presupune că stațiile de lucru se conectează automat și dinamic la VLAN, în funcție de aplicație, ID-ul utilizatorului sau alte politici predefinite de către administrator.

10.3. VLAN Trunking Protocol (VTP)[1]

Procesul prin care unui cadru al unei rețele i se adaugă un antet pentru a identifica cărui VLAN aparține se numește *VLAN tagging* (urmărirea VLAN-ului). În documentațiile CISCO acest proces este denumit *trunking*.

Pentru Ethernet, CISCO oferă două opțiuni în ceea ce privește *trunking*-ul : ISL și IEEE 802.1Q. ISL (Inter-Switch Link) urmărește cadrele folosind o opțiune proprietară CISCO în timp ce IEEE 802.1Q modifică antetul Ethernet prin adăugarea unui identificator pentru fiecare VLAN creat.

---

1. Pentru detalii, vizitați http : //www.cisco.com/warp/public/473.

VTP este un protocol de nivel doi care asigură consistența VLAN-urilor prin crearea unui domeniu comun de administrare. Acest protocol gestionează adăugarea, ștergerea, modificarea VLAN-urilor între mai multe switch-uri.

Configurațiile se realizează pe un singur switch numit *server vtp* și sînt propagate prin legături de tip trunchi (*trunk*) către toate switch-urile din cadrul aceluiași domeniu.

VTP poate opera în trei moduri :

- *Server.* Serverele pot crea, modifica sau șterge VLAN-uri precum și alți parametri de configurare pentru un domeniu vtp.
- *Client.* Switch-urile care funcționează ca și clienți vtp vor primi informațiile necesare de la server (un switch) fără a necesita prea multe configurări individuale.
- *Transparent.* Un switch care funcționează în acest mod nu transmite informațiile cu privire la modificările efectuate asupra sa și celorlalte switch-uri din domeniu. Aceste modificări afectează doar switch-ul respectiv.

Pentru că prea multă teorie fără practică nu folosește, ne-am gîndit ca în cele ce urmează să exemplificăm partea de switching.

Înainte de a trece la fapte, se cuvine să facem cîteva mențiuni. În primul rînd, ne bazăm pe experiența acumulată în cadrul rețelei FEAA : aproximativ 400 de stații, 12 servere, o duzină de switch-uri și un rest de hub-uri. În al doilea rînd, switch-urile folosite sînt Catalyst-uri de la CISCO (din seria 1900 și 2950), motiv pentru care în exemplele ce vor urma vom prezenta facilitățile acestor produse. În al treilea rînd, nu pretindem că le știm pe toate.

Familia de switch-uri Catalyst de la CISCO începe cu seria 1900 și continuă cu 2950, 3500XL, 4000, 5000 și 6000. Facilitățile (și prețurile ! ! !) variază de la un model la altul, dar majoritatea switch-urilor au propriul sistem de operare (IOS – *Internetworking Operating System*).

Un switch din seria 1900[1] poate fi configurat în trei moduri :

- De la o consolă prin intermediul unui meniu.
- Prin intermediul browserului (*Web based Visual Switch Manager* – VSM[2]).
- Dintr-o fereastră comandă (CLI – *Command Line Interface*).

Ne vom îndrepta atenția asupra variantei de configurare CLI, deoarece varianta browserului nu oferă toate facilitățile de care ar avea nevoie un administrator. Înainte de a prezenta principalele comenzi ale IOS, trebuie spus că la pornirea switch-ului, acesta afișează anumite valori implicite în funcție de model. Pentru un switch 1900, cele mai importante sînt :

- IP address : 0.0.0.0 ;
- CDP : enabled ;
- Switching mode : FragmentFree ;

---

1. Aceste modele sînt depășite ca performanțe, deoarece au doar cîte două porturi pentru legături de tip trunk, ceea ce pentru o rețea mai mare poate constitui un mare dezavantaj. Pentru noi, momentan, este de ajuns.
2. În funcție de modelul de switch deținut, softul poate fi descărcat de la adresa http ://www.cisco.com/public/sw-center/sw-lan.shtml.

- 100BaseT port : Autonegotiate duplex mode ;
- 10BaseT port : Half duplex ;
- Spanning Tree : Enabled ;
- Console password : None.

10.4. Comenzile IOS[1]

Pentru cei care sînt familiarizaţi cu mediile tip Linux/Unix, navigarea la prompter este asemănătoare : cu tab se afişează prima comandă care începe cu litera tastată, iar cu săgeată-sus se apelează history-ul comenzilor tastate. Tastarea unei litere urmată de *?* apelează helpul. Mai pot fi folosite următoarele combinaţii :

- Ctrl+E – salt la sfîrşit de linie ;
- Ctrl+A – un caracter înainte ;
- Ctrl+B – un caracter înapoi ;
- Ctrl+P – repetă ultima comandă ;
- Show history – afişează ultimele 10 comenzi.

Pentru a se evita accesul neautorizat la facilităţile switch-ului, trebuie configurate parolele de acces. Activarea modului de configurare globală se face prin comanda *enable*, urmată de activarea terminalului *config t* :

```
>enable
#config t
Enter configuration commands, one per line. End with CNTL/Z.
(config)#
```

Activarea parolei se face prin *enable password* :

```
(config)#enable password?
level Set exec level password
(config)#enable password level?
<1-15> Level number
```

Pentru activarea modului de configurare *utilizator* se foloseşte Level1. Pentru modul *configurare* se foloseşte Level 15.

```
(config)#enable password level 1 <parola>
(config)#enable password level 15 <parola>
(config)#exit
```

1. Lista completă a comenzilor suportate de un switch o găsiţi pe site-ul CISCO. Facem menţiunea că, în funcţie de modelul şi versiunea IOS instalată pe switch, aceste comenzi pot fi diferite. În exemplul nostru, IOS-ul switch-ului este *enterprise edition*. În cazul unui swich din seria 2950, apar cîteva modificări, ca urmare şi a facilităţilor oferite (DNS ; DHCP etc).

Vizualizarea configurației de pe switch se face cu *show running-config* sau *show run* :

```
Current configuration:
enable secret 5 $1$upKn$KepmokI3NvkFVB6AnOcn0/
enable password level 1 "ADIM"
enable password level 15 "ADIM1"
!
interface Ethernet 0/1
!
interface Ethernet 0/2
!
interface Ethernet 0/3
!
interface Ethernet 0/4
!
```

Pentru setarea numelui switch-ului, din modul de configurare se folosește comanda *hostname* :

```
 (config)#hostname 1900A
1900(config)#
```

Din acest moment, numele switch-ului va preceda prompterul. La instalare, switch-ul nu cunoaște nici o adresă IP sau alte informații de acest gen. Aceste setări implică aceleași operații ca și în cazul unui calculator obișnuit. Cu ajutorul comenzii *show ip* afișați informații despre setările ip.

```
1900#sh ip
IP Address: 0.0.0.0
Subnet Mask: 0.0.0.0
Default Gateway: 0.0.0.0
Management VLAN: 1
Domain name:
Name server 1: 0.0.0.0
Name server 2: 0.0.0.0
HTTP server : Enabled
HTTP port : 80
```

Pentru setarea adresei IP[1] (urmată de subnet mask) se folosește comanda *ip address* ; pentru gateway, *ip default-gateway* :

```
1900(config)#ip address 172.16.10.2 255.255.255.0
1900(config)#ip default-gateway 172.16.10.1
```

1. În cazul switch-urilor 2950, acest lucru trebuie realizat pe o rețea VLAN administrativă.

Pentru configurarea porturilor unui switch se lucrează în modul global. Se foloseşte ıanda *interface* sau varianta scurtă *int* :

```
1900#config t
Enter configuration commands, one per line. End with CNTL/Y
1900(config)#int ethernet?
<0-0> IEEE 802.3
```

Mesajul de mai sus indică faptul că switch-ul nu are sloturi disponibile. Pentru ·area porturilor se foloseşte aceeaşi comandă urmată de un slash (/) :

```
1900#config t
Enter configuration commands, one per line. End with CNTL/Y
1900(config)#int ethernet 0/?
<1-25> IEEE 802.3
```

Pentru a începe configurarea unui port comanda va fi :

```
1900A(config)#int ethernet 0/1
```

În acest moment se va schimba şi promptul consolei de configurare :

```
1900(config-if)#?
Interface configuration commands:
cdp             cdp interface subcommands
description     Interface specific description
duplex          configure duplex operation
exit            exit from interface configuration mode
help            description of the interactive help system
no              negate a comand or set its defaults
port            perform switch port configuration
shutdown        shutdown the selected interface
spantree        spanning tree subsystem
vlan-membershyp VLAN membershyps configuration
```

Cum un switch poate să aibă atît porturi Ethernet, cît şi Fast Ethernet, se vor folosi nenzi diferite. Pentru configurarea unui port Fast Ethernet, se foloseşte comanda *ːrface fast ethernet :*

```
1900(config)#int fastEthernet?
<0-0> FastEthernet IEEE 802.3
1900(config)#int fastEthernet 0/?
<26-27> FastEthernet IEEE 802.3
1900(config)#int fastEthernet 0/26
1900(config-if)#int fast 0/26
```

După ce ați schimbat configurația implicită a switch-ului, verificați modificările cu ajutorul comenzii *show interface*:

```
1900#show int e0/1
Ethernet 0/1 is Suspended-no-linkbeat
Hardware is Built-in 10Base-T
Address is 0030.80CC.7D01
MTU 1500bytes, BW 10000 Kbits
802.1d STP state: Forwarding Forward Transitions: 1
. . . . . . . . . . . . . . . . . . . . . . . . .
1900#show int f0/26
FastEthernet 0/26 is Suspended-no-linkbeat
Hardware is Built-in 100Base-TX
Address is 0030.80CC.7D1A
MTU 1500bytes, BW 100000 Kbits
802.1d STP state: Forwarding Forward Transitions: 0
```

Pentru a nu uita ce conexiune există pe o interfață/port, este bine să facem o scurtă descriere a acesteia. Din modul de configurare al acesteia se folosește comanda *description*:

```
1900(config)#int e0/1
1900(config-if)#description VLAN_Contabilitate
1900(config-if)#int f0/26
1900(config-if)#description trunk_la_Corpul_B
```

Spuneam că numărul și tipul porturilor disponibile pe un switch diferă de la un model la altul. Pentru activarea modului duplex se folosește comanda cu același nume din modul de configurare a interfeței.

```
1900(config)# int f0/26
1900(config-if)#duplex?
auto                Enable auto duplex configuration
full                Force full duplex configuration
full-flow-control   Force full duplex with flow control
half                Forece half duplex operation
```

Parametrii de mai sus au următoarea semnificație:

- *Auto* – setează portul în modul de lucru autonegociere. Este setat implicit pentru porturile 100BaseTX.
- *Full* – forțează lucrul în modul full-duplex pentru porturile pe 10 sau 100Mbps.
- *Full-flow-control* – este valabilă numai pentru porturile 100BaseTX.
- *Half* – Setarea implicită pentru porturile 10BaseT, forțează porturile să lucreze numai în acest mod.

Dacă se dorește ștergerea configurației introdusă și revenirea la setările producătorului, se folosește comanda *delete*:

```
1900# delete?
nvram     NVRAM configuration
vtp       Reset VTP configuration to defaults
1900(config)# delete nvram
Reset system with factory defaults, [Y]es or [N]o? Yes
```

Pentru configurarea unei VLAN pe un switch cu sistem de operare, se foloseşte comanda *vlan*.

```
1900(config)#vlan 2 name Contabilitate
1900(config)#vlan 3 name Vinzari
1900(config)#vlan 4 name IT
```

După crearea VLAN-urilor, se foloseşte comanda *show vlan* pentru a vizualiza informaţiile configurate pentru vlan.

```
1900#     show vlan
VLAN      Name                 Status      Ports
- - - - - - - - - - - - - - - - - - - - - - - - - - -
1         default              Enabled     1-12, AUI, A, B
2         Contabilitate        Enabled
3         Vinzari              Enabled
4         IT                   Enabled
1002      fddi-default         Suspended
1003      token-ring-defau     Suspended
1004      fddinet-default      Suspended
1005      trnet-default        Suspended
```

Fiecare port al switch-ului poate fi configurat în continuare ca membru al unui vlan cu ajutorul comenzii *vlan-membership*.

```
1900(config)# int e0/2
1900(config-if)#vlan-membership?
  dynamic Set VLAN membership type as dynamic
  static Set VLAN membership type as static
1900(config-if)#vlan-membership static 2
1900(config-if)#int e0/4
1900(config-if)#vlan-membership static 3
1900(config-if)#int e0/5
1900(config-if)#vlan-membership static 4
1900(config-if)#exit
```

Pentru a vizualiza maniera de alocare a porturilor pe VLAN-uri folosiţi *show vlan* sau *show vlan-membership*.

Legăturile **trunk** sînt legături pe 100 sau 1000Gbps între două dispozitive: switch--switch, switch-router. O interfaţă poate suporta o legătură tip *trunk* doar dacă este

activă (setată pe *on* sau *desirable*) şi dacă există un dispozitiv conectat. Dacă dispozitivul conectat este on, desirable sau auto, va încerca să treacă portul pe legătură tip trunk.

Pentru a se verifica starea unei interfeţe se foloseşte comanda *show trunk*:

```
1900(config)#int f0/26
1900(config-if)#trunk?
       auto            Set DISL state to AUTO
       desirable       Set DISL state to DESIRABLE
       nonegotiate     Set DISL state to NONEGOTIATE
       off             Set DISL state to OFF
       on              Set DISL state to ON
1900(config-if)#trunk on
```

Majoritatea switch-urilor cu management sînt configurate implicit ca servere vtp. Vom configura, în continuare, un switch ca server vtp pentru domeniul *test*:

```
1900(config)#vtp?
client                  vtp client
domain                  Set VTP domain name
password                Set VTP password
pruning                 VTP pruning
server                  VTP server
transparent             VTP transparent
trap                    VTP trap
1900(config)#vtp server
1900(config)#vtp domain test
```

```
1900A#show vtp
Configuration revison 0
Maximum VLANs supported locally: 1005
VTP domain name          :test
VTP password               :
VTP operating mode         :server
VTP pruning mode         :Disabled
VTP traps generation     :Enabled
Configuration last modified by: 0.0.0.0 at 00-00-0000 00:00:00
```

10.5. Exemplu

Aşa stînd lucrurile, ipoteza de lucru este prezentată în figura următoare şi implică configurarea switch-urilor astfel încît cele două servere să facă parte din două VLAN-uri.

Primul lucru cu care trebuie să începem se referă la alocarea porturilor switch-urilor din schemă.

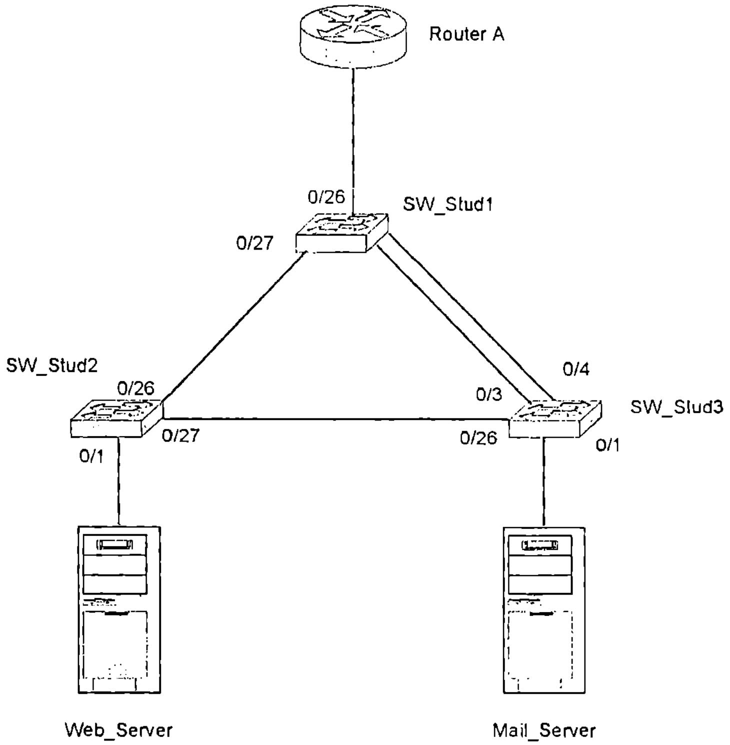


Figura 10.5.1. Reţea

Switch-urile din seria 1900 au doar două porturi pe 100Mbps. Atît ISL, cît şi 802.1Q necesită pentru legăturile de tip trunk (legături switch-la-switch sau switch-la router) porturi pe 100Mbps. Prin urmare, legătura dintre Router A şi SW_Stud1 va folosi unul din porturile pe 100Mbps ale switch-ului. Pentru conectarea acestuia la SW_Stud2, se va folosi ultimul port pe 100Mbps, iar pentru SW_Stud3, se vor folosi două porturi pe 10Mbps deoarece avem nevoie de două VLAN-uri. Nu uitaţi: legăturile de tip trunk nu sînt permise pe porturi la 10Mbps. Am ales acest model pentru a scoate în evidenţă cît de importantă este scalabilitatea în proiectarea unei reţele.

Vom începe cu SW_Stud1.

Pentru activarea consolei switch-ului din meniu se va alege opţiunea *K*.

Pentru a se evita accesul neautorizat la facilităţile switch-ului, trebuie configurate parolele de acces. Pot fi configurate două parole (*enable password*), una pentru modul de lucru utilizator (se foloseşte Level 1) şi una pentru accesul în modul configurare (Level 15). Parolele trebuie să aibă minimum 4 caractere şi maximum 8[1].

1. Dacă uitaţi parolele vizitaţi *www.cisco.com* pentru a afla cum mai puteţi accesa respectivul switch.

```
(config)#enable password level 1 pentax1
(config)#enable password level 15 pentax15
(config)#exit
```

În continuare, vom configura numele acestui switch (*hostname <nume switch>*), adresa ip (*ip address <adresa ip subnet mask>*), gateway-ul[1] (*ip default-gateway*) și porturile/interfețele (*interface*):

```
(config)#hostname SW_Stud1
SW_Stud1(config)#sh ip
IP Address: 0.0.0.0
Subnet Mask: 0.0.0.0
Default Gateway: 0.0.0.0
Management VLAN: 1
Domain name:
Name server 1: 0.0.0.0
Name server 2: 0.0.0.0
HTTP server : Enabled
HTTP port : 80
```

```
SW_Stud1(config)#ip address 172.16.10.2 255.255.255.0
SW_Stud1(config)#ip default-gateway 172.16.10.1
SW_Stud1(config)#interface fastEthernet 0/?
<26-27> FastEthernet IEEE 802.3
SW_Stud1(config-if)#int fast 0/26
SW_Stud1(config-if)#description trunk_la_RouterA
SW_Stud1(config-if)#trunk on
SW_Stud1(config-if)#int fast 0/27
SW_Stud1(config-if)#description trunk_la_SW_Stud2
SW_Stud1(config-if)#trunk on
SW_Stud1(config-if)#interface ethernet0/3
SW_Stud1(config-if)#description Legatura_la_SW_Stud3
SW_Stud1(config-if)#interface ethernet0/4
SW_Stud1(config-if)#description Legatura_la_SW_Stud3
```

Activarea modului duplex pentru porturile Fast Ethernet:

```
SW_Stud1(config)#int f0/26
SW_Stud1(config)#duplex full
SW_Stud1(config)#int f0/27
SW_Stud1(config)#duplex full
```

Pe switch-ul SW_Stud1 vom crea domeniul VTP (*vtp domain <nume_domeniu>*):

1. Adresa IP a interfeței routerului la care se conectează.

```
SW_Stud1(config)#vtp domain Studenti
SW_Stud1(config)#vtp server
```

Vom crea pe acest switch două VLAN-uri; Web și Mail (*vlan <număr> name<nume>*) și vom asocia (*vlan-membership static <număr vlan>*) porturile 3 și 4 acestor VLAN-uri:

```
SW_Stud1(config)#vlan 2 name Web
SW_Stud1(config)#vlan 3 name Mail
SW_Stud1(config)#interface ethernet 0/3
SW_Stud1(config-if)#vlan-membership static 2
SW_Stud1(config)#interface ethernet 0/4
SW_Stud1(config-if)#vlan-membership static 3
```

Cu ajutorul comenzilor *show vlan* sau *show vlan-membership* vom verifica informațiile referitoare la VLAN-urile create.

```
SW_Stud1#sh vlan
VLAN  Name                 Status     Ports
-----------------------------------------------
1     default              Enabled    1-2,5-12, AUI, A, B
2     web                  Enabled    3
3     mail                 Enabled    4
1002  fddi-default         Suspended
1003  token-ring-default   Suspended
1004  fddinet-default      Suspended
1005  trnet-default        Suspended
```

Ne mutăm acum la switch-ul SW_Stud2 pentru care cea mai mare parte a configurării este identică cu SW_Stud1. Conform schemei, acest switch se conectează la SW_Stud1 prin portul Fast Ethernet 26 și la SW_Stud3 prin portul Fast Ethernet 27. Portul Ethernet 1 trebuie configurat ca membru în VLAN-ul 2 (Web.).

```
>enable
#config t
Enter configuration commands, one per line. End with CNTL/Z.
config)#hostname SW_Stud2
SW_Stud2(config)#enable password level 1 pentax1
SW_Stud2(config)#enable password level 15 pentax15
SW_Stud2(config)#ip address 172.16.10.3 255.255.255.0
SW_Stud2(config)#ip default-gateway 172.16.10.1
SW_Stud2(config-if)#int fast 0/26
SW_Stud2(config-if)#description trunk_la_SW_Stud1
SW_Stud2(config-if)#trunk on
SW_Stud2(config-if)#int fast 0/27
SW_Stud2(config-if)#description trunk_la_SW_Stud3
```

```
SW_Stud2(config-if)#trunk on
SW_Stud2(config-if)#interface ethernet0/1
SW_Stud2(config-if)#description Legatura_la_Web_Server
SW_Stud2(config-if)#exit
SW_Stud2(config)#vtp domain Studenti
SW_Stud2(config)#vtp client
SW_Stud2(config)#interface ethernet0/1
SW_Stud2(config-if)#vlan-membership static 3
```

Lucrurile sînt ceva mai delicate în cazul SW_Stud3, pentru că trebuie asociate corect porturile în funcție de VLAN-urile create. Portul Ethernet 3 face parte din VLAN-ul 2, iar portul Ethernet 4 din VLAN-ul 3. Portul Ethernet 1 prin care se conectează Mail serverul face parte tot din VLAN-ul 3.

```
>enable
#config t
Enter configuration commands, one per line. End with CNTL/Z.
config)#hostname SW_Stud3
SW_Stud3(config)#enable password level 1 pentax1
SW_Stud3(config)#enable password level 15 pentax15
SW_Stud3(config)#ip address 172.16.10.4 255.255.255.0
SW_Stud3(config)#ip default-gateway 172.16.10.1
SW_Stud3(config-if)#int fast 0/26
SW_Stud3(config-if)#description trunk_la_SW_Stud2
SW_Stud3(config-if)#trunk on
SW_Stud3(config-if)#interface ethernet0/3
SW_Stud3(config-if)#description Legatura_la_SW_Stud1
SW_Stud3(config-if)#interface ethernet0/4
SW_Stud3(config-if)#description Legatura_la_SW_Stud1
SW_Stud3(config-if)#exit
SW_Stud3(config)#vtp domain Studenti
SW_Stud3(config)#vtp client
SW_Stud3(config)#interface ethernet0/3
SW_Stud(config-if)#vlan-membership static 2
SW_Stud3(config)#interface ethernet0/4
SW_Stud(config-if)#vlan-membership static 3
SW_Stud3(config)#interface ethernet0/1
SW_Stud(config-if)#vlan-membership static 2
```

Pentru ca cele două servere să se poată „vedea” în afara VLAN-urilor din care fac parte, ar trebui ca pe routerul din schemă să mai configurăm și tipul de rutare pentru exemplul ales. Dar despre acest subiect vom discuta în capitolele următoare.

CAPITOLUL 11

Privire generală asupra routerelor

Routerul are aceleaşi componente ca PC-ul : procesor, memorie, interfeţe şi magistrală. Poate fi asemuit unui calculator care este dedicat executării unei sarcini mai speciale : rutarea informaţiilor în reţele.

Ca şi în cazul calculatoarelor, care au nevoie de un sistem de operare pentru a putea rula aplicaţii clasice, şi routerul are nevoie de un astfel de sistem de operare care nu este nici Linux, nici Unix, nici măcar Windows. Sistemul de operare al routerului se numeşte, ca şi la switch-uri, *Internetworking Operating Software (IOS)* şi foloseşte la rularea fişierelor de configurare ale routerului. Prin intermediul acestor fişiere se controlează traficul dintre routere, control care se bazează pe protocoalele de rutare prin intermediul cărora se direcţionează protocoalele rutabile şi tabelele de rutare.

Pentru ca toate acestea să aibă loc, routerul trebuie configurat aşa cum se configurează orice alt calculator (aproape).

11.1. Componentele routerului şi moduri de configurare

Tehnic vorbind, routerul este un calculator care selectează cel mai bun traseu (path) şi gestionează comutarea pachetelor între două reţele diferite. Un router poate fi configurat în mai multe moduri :

- de la un terminal în timpul instalării sale ;
- via un modem, folosind un port auxiliar ;
- de la un terminal virtual (VT0-4), după ce a fost instalat în reţea ;
- de pe un server TFTP din reţea.

Să vedem, în continuare, care sînt componentele interne ale unui router :

- *RAM/DRAM* – reprezintă memoria în care se păstrează tabelele de rutare, cache-ul ARP, fast switching cache-ul şi „coada" pe care o formează pachetele ce urmează a fi rutate. RAM oferă, de asemenea, memoria de lucru necesară (chiar dacă sună a pleonasm) fişierelor de configurare a routerului. *În momentul întreruperii alimentării cu tensiune a routerului sau restartării acestuia, conţinutul RAM se pierde ! ! !*

- *NVRAM* – Memorie RAM nonvolatilă, păstrează fişierele startup/backup ale routerului. După cum îi spune şi numele, nu se pierde dacă routerul nu mai este alimentat cu tensiune.
- *Flash* – memorie ROM reprogramabilă, păstrează imaginea sistemului de operare şi microcodul acestuia. Permite actualizarea software-ului fără a se schimba chipurile procesorului. Poate păstra versiuni diferite ale sistemului de operare.
- *ROM* – conţine instrumente de diagnosticare, un program bootstrap şi sistemul de operare. Dacă se doreşte upgrade la IOS, trebuie înlocuite chip-urile microprocesorului.
- *Interfeţe* – reprezintă conexiunile reţelei prin care pachetele intră şi ies din router. Pot fi amplasate direct pe placa de bază sau în module separate.

La o primă vedere, cam aşa stau lucrurile. Cum însă RAM-ul este componenta cea mai importantă a routerului, trebuie să o privim cu mai multă atenţie.

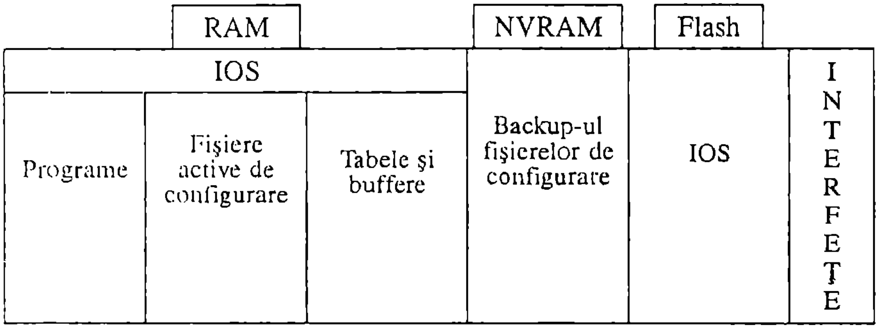


Figura II.1.1. Componentele routerului

Această memorie reprezintă principala zonă de lucru a unui router. La pornire, în memoria ROM se execută un program bootstrap ce realizează anumite teste şi încarcă IOS-ul în memorie (aveam în vedere IOS-ul folosit de routerele CISCO). Autoritatea executivă sau EXEC reprezintă una dintre componentele cele mai importante ale CISCO IOS. EXEC este cea care primeşte şi execută comenzile prin care administratorul configurează routerul.

Memoria RAM este folosită şi pentru păstrarea fişierului de configurare activă, a tabelelor ARP şi a tabelelor de rutare. Conţinutul fişierului de configurare poate fi afişat prin intermediul unui terminal sau al unei console. O versiune a acestui fişier este păstrată şi în NVRAM. Acest fişier este încărcat în memorie la fiecare iniţializare a routerului. Despre informaţiile conţinute de acest fişier vom discuta în paginile următoare.

Spre deosebire de fişierul de configurare, imaginea IOS nu poate fi afişată pe ecranul unui terminal. Această imagine este de obicei executată în memoria RAM. Sistemul de operare este organizat în rutine ce gestionează sarcinile asociate diferitelor protocoale: transferul datelor, gestiunea tabelelor şi a bufferelor, actualizarea tabelelor de rutare, executarea comenzilor introduse etc.

Indiferent de modul în care este accesat (de la o consolă, prin intermediul unei sesiuni Telnet), un router se poate afla în diferite moduri care să ofere funcţionalităţi diverse:

- Modul *user EXEC* - este modul în care un utilizator poate să vizualizeze anumite informaţii despre router, dar nu poate efectua nici o schimbare asupra stării acestuia.
- Modul *privileged EXEC* - este modul în care se pot introduce comenzi de testare şi debug, se poate examina în detaliu starea routerului, se poate lucra asupra fişierelor de configurare şi se pot accesa celelalte moduri de configurare.
- Modul *setup* - este modul care permite crearea primei configurări a routerului de la promptul unei console.
- Modul *global configuration* - este modul în care se obţine accesul la comenzile de configurare.
- Modul *RXBOOT* - este un mod de întreţinere care se foloseşte mai ales în cazul pierderii parolelor.
- Alte moduri de configurare: oferă opţiuni mai detaliate de configurare.

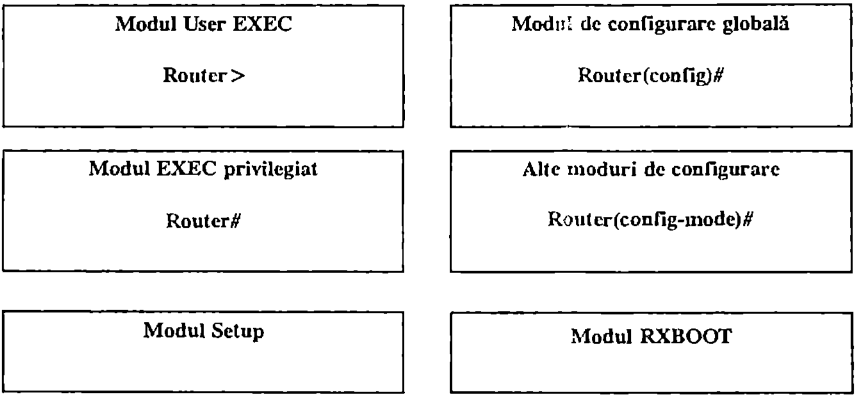


Figura 11.1.2. Moduri de configurare

11.2. Pornirea unui router

De ce credeţi că am prezentat comenzile de mai înainte şi abia acum discutăm despre setarea routerului?

Iniţializarea unui router presupune încărcarea programului bootstrap, a sistemului de operare şi a fişierului de configurare. Dacă routerul nu găseşte un fişier de configurare, trece automat în modul de lucru setup după care memorează în NVRAM o copie a noii configurări.

La pornire, routerul execută o rutină de autodiagnoză, denumită Power-On-Self-Test. În timpul acestei testări, asupra modelelor hardware se execută programele de diagnoză din ROM pentru a se verifică gradul de operabilitate al CPU, memoriei şi interfeţelor. Dacă totul este în regulă, routerul continuă cu iniţializarea sistemului de operare.

După POST, pe măsură ce se desfăşoară inițializarea routerului, au loc următoarele evenimente:

1. Se execută bootstrap-ul. Acesta este un program simplu prin care se încarcă instrucțiuni al căror efect este încărcarea în memorie a altor instrucțiuni care conduc spre modurile de configurare a routerului.
2. Se caută sistemul de operare după locația indicată în cîmpul boot din registrul de configurare.
3. Se încarcă imaginea sistemului de operare. După ce devine operațional, sistemul de operare localizează componentele hard şi soft pe care le listează la consolă.
4. Fişierul de configurare salvat în NVRAM este încărcat în memoria principală şi executat linie cu linie. Comenzile de configurare pornesc procesul de rutare, atribuie adresele interfețelor, setează caracteristicile mediilor de transmisie etc.
5. Dacă în NVRAM nu există nici un fişier de configurare valid, sistemul de operare execută o rutină de interogare denumită *setup dialog*.

Setup-ul este folosit pentru a oferi routerului o configurare minimă. Cu ajutorul comenzilor *show startup-config* şi *show running-config* se afişează cele două fişiere de configurare: activ, respectiv backup. Dacă se doreşte ştergerea backup-ului fişierului de configurare din NVRAM, se foloseşte comanda *erase startup-config*. Apoi, cu ajutorul comenzii *reload* se rebootează routerul, acțiune ce are ca efect reluarea întregului proces de startup. Pentru a se ajunge în modul de lucru setup, se tastează comanda cu acelaşi nume: *setup*.

Aminteam, cu cîteva rînduri mai înainte, că scopul *modului setup* este de a oferi routerului o configurație minimă în cazul în care nu găseşte informațiile necesare în alte surse. Majoritatea prompt-urilor din timpul configurării routerului prin comanda *setup* oferă răspunsul default între paranteze pătrate. Setup-ul se poate anula în orice moment cu Ctrl+C, toate interfețele fiind oprite.

După terminarea configurării, aceasta va fi afişată pe ecran o dată cu întrebarea dacă doriți să folosiți această configurare. Răspunsul „Yes" la această întrebare va avea ca efect executarea instrucțiunilor de configurare şi salvarea lor în NVRAM. Dacă răspundeți cu „No", configurarea nu va fi salvată şi procesul va reîncepe.

După vizualizarea unui sumar al interfeței curente, pe ecran este afişat promptul corespunzător introducerii parametrilor globali ai routerului. Aceşti parametri reprezintă valorile de configurare pe care le selectați.

Primul parametru global vă permite stabilirea unui nume de host pentru router. Acest nume va deveni parte a prompturilor IOS-ului de la CISCO pentru toate modurile de configurare. În timpul configurării inițiale, numele implicit al routerului va fi afişat între paranteze pătrate, [Router].

Următorul parametru global ce va fi folosit se referă la parolele utilizate pentru protejarea routerului. La început, trebuie introdusă o parolă validă („enable"). Algoritmul de criptare CISCO preia parola după ce a fost introdusă de la prompt („Enter enable secret"). Astfel, oricine ar lista conținutul fişierului de configurare de pe router nu va putea vizualiza parola în clar.

În timpul setup-ului se recomandă ca „enable password" (parola) să fie diferită de „enable secret word". Toate parolele sînt case sensitive şi pot conține caractere alfanumerice.

După ce se răspunde afirmativ la ultima întrebare din cadrul configurării inițiale, routerul este gata de utilizare.

11.3. Configurarea routerului

La startare, routerul foloseşte următoarele informaţii din cadrul fişierului de configurare:

- Versiunea Cisco a IOS-ului;
- Identificarea routerului;
- Locaţia (iile) fişierului folosit la bootare;
- Informaţii despre protocoale;
- Configurarea interfeţelor.

Dacă nu este disponibilă nici o configurare, se porneşte dialogul de configurare (*setup*).

Informaţiile privind configurarea routerului pot fi generate în mai multe moduri. În modul privilegiat EXEC se poate folosi comanda *configure* de la un terminal virtual sau o consolă. Această variantă permite modificări asupra unei configurări existente. Aceeaşi comandă se poate folosi pentru a încărca o configuraţie de pe un server TFTP. Iată, în continuare, cîteva dintre opţiunile disponibile la configurare.

- *configure terminal* – configurarea manuală a routerului de la un terminal;
- *configure memory* – încărcarea informaţiilor de configurare din memoria NVRAM;
- *copy tftp running-config* – încărcarea informaţiilor de configurare de pe un server TFTP în memoria RAM;
- *show running-config* – afişarea configurării curente în RAM;
- *copy running-config startup-config* – memorarea configurării curente din memoria RAM în NVRAM;
- *copy running-config tftp* – memorarea configurării curente din memoria RAM pe un server TFTP;
- *show startup-config* – afişarea configurării salvate în NVRAM;
- *erase startup-config* – ştergerea conţinutului NVRAM.

11.4. Accesul la alte routere

Este posibil ca în acest moment să vă întrebaţi ce şi cum se întîmplă cu routerele din imediata apropiere a routerului pe care îl administraţi voi.

Cisco Discovery Protocol (CDP) furnizează o comandă *show* proprietară, comandă ce permite administratorului să acceseze informaţii despre cum sînt configurate routerele conectate direct la routerul administrat. CDP rulează la nivelul legătură date, motiv pentru care echipamentele ce lucrează cu alte protocoale de nivel 3 pot afla unele de altele (vă amintiţi că adresele nivelului legătură date sînt similare adreselor MAC).

Cînd un router pe care rulează IOS (Release 10.3 sau mai nou) bootează, în mod automat se startează şi CDP. Acesta permite routerului să detecteze routerele aflate în vecinătatea sa, pe care rulează CDP.

Administratorul de reţea va folosi comanda *show cdp neighbors* pentru a afişa actualizările făcute de CDP pe router sau, altfel spus, despre reţelele conectate direct la respectivul router. Orice router pe care rulează CDP schimbă cu „vecinii" săi informaţii cu privire la protocoalele cu care lucrează.

Chiar dacă CDP rulează implicit la pornirea routerului, administratorul trebuie să activeze explicit acest protocol pentru fiecare din interfeţele routerului, folosind comanda *cdp enable*. Routerul păstrează informaţiile pe care le primeşte de la „vecini" într-o zonă de memorie cache. Dacă primeşte un cadru care indică schimbarea unei informaţii cu privire la respectivul vecin, routerul va înlocui informaţiile vechi cu cele noi.

Comanda *show cdp interface* afişează valorile pentru timerii CDP, starea interfeţei şi tipul încapsulării folosite de CDP. Valorile implicite ale timerilor sînt setate la 60 de secunde pentru frecvenţa actualizărilor, respectiv 180 de secunde pentru durata de viaţă a intrărilor CDP. Dacă routerul primeşte o actualizare mai devreme decît este stabilit prin timer sau dacă durata de viaţă a expirat, renunţă la vechile informaţii.

Cu ajutorul comenzii *show cdp entry <nume router>* se va afişa conţinutul memoriei cache aferente unei singure intrări CDP, inclusiv toate adresele de nivel 3 prezente în routerul specificat.

Pentru a vizualiza update-urile recepţionate de routerul local, se foloseşte comanda *show cdp neighbors*.

11.5. Protocoale pentru rutare

Există trei metode prin care un router *învaţă* traseul unui pachet către destinaţie:

- rute statice – sînt definite manual de către administratorul de reţea sub forma următorului *hop* (următorul router sau gateway) către destinaţie. Sînt folosite mai ales în reţelele mici, cînd se doreşte reducerea traficului. ;
- rute implicite – sînt definite manual de către administratorul de reţea sub forma traseului pe care îl urmează un pachet, atunci cînd nu se cunoaşte calea către destinaţie ;
- rute dinamice – routerul învaţă traseele către destinaţie prin recepţionarea actualizărilor oferite de alte routere din reţea.

Identificarea traseului pe care trebuie să îl urmeze un pachet este funcţia routerului prin care acesta evaluează traseele către destinaţie şi care dintre acestea este cel mai bun. Rutarea se referă la procesul prin care se alege cel mai bun traseu pentru transmiterea pachetelor către destinaţie.

Toate protocoalele pentru rutare au acelaşi obiectiv : partajarea informaţiilor despre reţea între routerele participante. Acest obiectiv este însă atins în moduri diferite. Unele protocoale transmit tabele de rutare între routere, în timp ce altele transmit informaţii doar despre conexiunile directe pe care le gestionează. Deosebirile nu se limitează numai la cele menţionate anterior. Caracteristicile cu privire la performanţe şi scalabilitate sînt diferite de la un protocol la altul.

Protocoale distance-vector (vector-distanţă)

În categoria protocoalelor distance-vector (şi derivatele acestora) sînt incluse :

- **RIP- Routing Information Protocol, versiunile 1 şi 2** ;
- **IGRP - Interior Gateway Routing Protocol** ;
- **RTMP - AppleTalk Routing Table Maintenance Protocol** ;
- **AURP - AppleTalk Update-Based Routing Protocol** ;
- **EIGRP - Enhanced IGRP** ;
- **BGP - Border Gateway Protocol.**

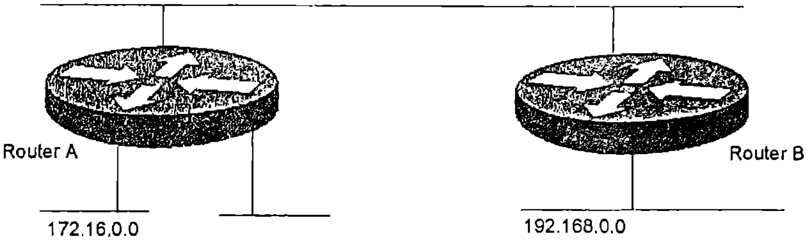
Ce înseamnă de fapt vector-distance? Termenul se referă la direcţia (şi informaţiile aferente) pe care trebuie să o parcurgă pachetele pînă la destinaţie, direcţie exprimată de cele mai multe ori sub forma de *hop count*-uri. Hop count reprezintă numărul routerelor care trebuie traversate de un pachet pentru a ajunge la reţeaua destinaţie (pentru unele protocoale această unitate de măsură se referă la numărul legăturilor).

Un protocol distance-vector întreţine şi transmite tabele de rutare în care sînt listate toate reţelele cunoscute şi distanţele către fiecare dintre acestea. O tabelă de rutare arată cam aşa :

Reţea	Distanţa în hop-uri	Hop-ul următor
10.0.0.0	0 (conexiune directă)	Interfaţa 1
172.16.0.0.	0 (conexiune directă)	Interfaţa 2
172.17.0.0.	1	172.16.0.2.
172.18.0.0.	2	172.16.0.2.
192.168.1.0	1	10.0.0.2
192.168.2.0	2	10.0.0.2

Protocolul pentru rutare transmite o astfel de tabelă tuturor routerelor către care există o conexiune directă. Tabela de rutare îmbracă forma unui packet broadcast care este transmis la anumite intervale de timp. Dacă protocolul de rutare suportă tehnica denumită *split horizon,* routerul transmite doar rutele care pot fi atinse. Această tehnică reduce intervalul la care trebuie făcută actualizarea tabelelor de rutare şi creşte acurateţea informaţiilor despre rutare. Mai mult, informaţiile care pot fi gestionate mai bine local de către un router nu vor fi transmise celorlalte routere.

O altă tehnică implementată de aceste protocoale se referă la *hold down timer*: maniera standard prin care routerul încearcă să rezolve problema buclelor. Pentru a fi mai clari, vom exemplifica pe cele două reţele din imaginea următoare.



Reţeaua	Distanţa	Următorul hop
172.16.0.0	0	Interfaţa 1
192.168.2.0	1	Router B

Reţeaua	Distanţa	Următorul hop
192.168.2.0	0	Interfaţa 1
172.16.0.0	1	Router A

Cînd routerul își transmite tabela de rutare, el distribuie doar informațiile cu privire la rețeaua și distanța pînă la acea rețea, nu și următorul hop. Acesta este motivul pentru care apar buclele. Secvența unui eveniment care poate conduce la o rutare în buclă este cam așa:

1. Conexiunea routerului A la rețeaua 172.16.0.0 pică.
2. Routerul A șterge din tabela de rutare informațiile cu privire la rețeaua 172.16.0.0.
3. În baza informațiilor precedente obținute de la routerul A, routerul B își transmite tabela de rutare anunțînd că poate găsi rețeaua 172.16.0.0.
4. Routerul A adaugă în tabela de rutare rețeaua 172.16.0.0 cu distanța 2 și următorul hop routerul B.
5. Routerul A primește un cadru de la un calculator din rețeaua 172.16.0.0.
6. Routerul A transmite cadrul routerului B.
7. Routerul B transmite cadrul routerului A.
8. Se continuă pînă cînd valoarea TTL din cadru expiră.

Dacă nu ar exista mecanismul split horizon, problemele s-ar complica și mai mult. La un moment dat, routerul A va transmite o actualizare a rutelor sale prin care anunță că poate ajunge în rețeaua 172.16.0.0. Ca urmare, routerul B va actualiza ruta respectivă cu o distanță egală cu 3. Ambele routere vor continua să-și trimită actualizări pînă cînd cîmpul distanță ajunge la o valoare infinită (16 în cazul RIP-ului). În acest moment, routerul șterge respectiva rută din tabelă.

Problema actualizării informațiilor de către router este cunoscută sub denumirea *count-to-infinity*. Funcția hold down este cea care spune routerului să nu adauge în tabela de rutare informații despre o rută care a fost modificată, pînă cînd nu expiră timpul pentru hold-down.

În cazul nostru, dacă routerul A face apel la această funcție, nu va adăuga ruta pentru rețeaua 172.16.0.0. trimisă de routerul B. Acest lucru se întîmplă și dacă routerul B face apel la split horizon, pentru că nu va transmite routerului A informații despre rețeaua 172.16.0.0.

Protocoale link state (starea legăturii)

Această categorie de protocoale pentru rutare nu schimbă între ele tabele de rutare sub forma prezentată anterior. Informațiile transmise de routere vizează starea legăturilor (rețelelor) conectate direct. Routerul care folosește un astfel de protocol transmite periodic un pachet multicast prin care oferă informații despre starea conexiunilor sale. Routerele care primesc acest pachet îl vor transmite mai departe routerelor conectate direct.

Se includ în această categorie următoarele protocoale:

- **OSPF - Open Shortest Path First**;
- **IS-IS - Intermediate System - to - Intermediate - System**;
- **NLSP - NetWare Link Services Protocol.**

În general, convergența realizată de aceste protocoale este mult mai rapidă față de protocoalele distance-vector, dar acest avantaj are în spate puterea crescută a procesoarelor

şi memoriei de care trebuie să dispună routerul. La cele spuse anterior se mai adaugă uşurinţa cu care poate fi administrat un protocol distance-vector faţă de unul link-state.

Unităţi de măsură, ierarhii şi convergenţă

Pentru a determina ruta pe care trebuie transmis un pachet, protocoalele de rutare fac apel la diferite unităţi de măsură. În mod obişnuit, protocoalele de tip distance-vector folosesc după cum am pomenit deja, *hop count*-ul. Protocoalele mai noi pot calcula rutele ţinînd cont şi de alte caracteristici ale reţelei: întîrzierea, lăţimea de bandă disponibilă etc. Scalabilitatea unei reţele este direct afectată de unităţile de măsură folosite. De exemplu, un protocol precum RIP-ul poate să nu selecteze o rută cu o lăţime de bandă mai bună, dar care depăşeşte limita de 15 hop count-uri.

Chiar dacă toate routerele îndeplinesc aceleaşi sarcini, anumite protocoale nu suportă ierarhii. Protocoalele din această categorie grupează routerele în zone de lucru, sisteme autonome sau domenii de lucru. Într-o astfel de organizare, unele routere comunică cu cele din zona locală, în timp ce altele au ca sarcină interconectarea domeniilor sau sistemelor autonome.

Dacă privim protocoalele prin prisma locaţiei în care sînt folosite, le putem împărţi în două categorii: de interior şi de exterior.

Protocoalele de interior (RIP, OSPF, IGRP) sînt folosite de routerele din cadrul aceleiaşi organizaţii sau sistem autonom (sistem autonom = grup de routere aflat sub o administrare centralizată). La polul opus, protocoalele de exterior (BGP) rutează între diferite sisteme autonome.

O altă caracteristică a protocoalelor de rutare vizează maniera de tratare a adreselor IP. Protocoalele de rutare de tip *classful* (RIP v.1, IGRP) calculează lungimea prefixului (porţiunea network) unei adrese pentru a determina din ce clasă face parte. Un astfel de protocol nu transmite nici o informaţie cu privire la lungimea prefixului calculat. Notaţia care se foloseşte tot mai des în acest caz este următoarea: 10.1.0.1/16. Acest lucru înseamnă că prefixul reţelei are o lungime de 16 biţi, ceea ce înseamnă o mască de reţea cu valoarea 255.255.0.0.

Protocoalele de rutare de tip *classless* (RIP v.2, EIGRP, OSPF, BGP, IS-IS) transmit lungimea prefixului împreună cu adresa IP. În această manieră, reţelele pot fi grupate sub forma unei singure intrări în tabela de rutare, folosind lungimea prefixului pentru a specifica care reţele au fost grupate.

Convergenţa se referă la timpul necesar unui router pentru a înţelege de o manieră consistentă topologia unei reţele, atunci cînd au avut loc schimbări în cadrul acesteia. Prin schimbări în cadrul unei reţele vom înţelege segmentări, defectarea unui router, adăugarea unui router etc. Convergenţa este o componentă critică în cadrul proiectării unei reţele.

Acest proces este iniţiat cînd routerul este notificat că o legătură către unul dintre routerele pereche devine inactivă (de exemplu). Un router de la CISCO transmite cadre *keepalive* la fiecare 10 secunde pentru a determina starea unei legături.

Într-o reţea WAN, routerul transmite aceste cadre către routerul aflat la capătul unei legături, în timp ce într-o reţea LAN, aceste cadre sînt transmise către o adresă multicast.

11.6. RIP - Routing Information Protocol[1]

RIP a fost primul protocol standardizat dezvoltat pentru mediile TCP/IP. După cum aminteam şi mai devreme, acesta este un protocol de tip *distance-vector* destul de uşor de utilizat şi administrat.

Acest protocol transmite broadcast tabela sa de rutare la fiecare 30 de secunde. Un pachet poate să conţină pînă la 25 de rute, ceea ce pentru reţele mari reprezintă un dezavantaj. Pentru reţelele care vor folosi acest protocol trebuie ţinut cont de faptul că foloseşte hop count-ul ca unitate de măsură (maxim 15 routere) chiar dacă alte rute au o lăţime de bandă mai bună, congestie redusă etc.

IETF a dezvoltat cea de a doua versiune a acestui protocol prin care unele dintre problemele legate de scalabilitate au fost rezolvate. RIP versiunea 2 adaugă următoarele cîmpuri intrărilor din tabela de rutare:

- **Route tag** - un indicator care face diferenţa între rutele interne din cadrul domeniului RIP şi rutele externe care au fost importate de la alte protocoale de rutare sau de la sisteme autonome diferite.
- **Subnet mask** - conţine masca de reţea care va fi aplicată prefixului din cadrul adresei IP.
- **Next hop** - specifică adresa IP a următorului router către care va fi transmis pachetul.

Cîmpul *route tag* este cel care uniformizează reţelele ce folosesc RIP cu cele non-RIP. Faptul că în versiunea 2 a fost adăugat şi cîmpul subnet mask oferă suport pentru rutarea de tip classless. Mai multe detalii în RFC 1723.

11.7. IGRP - Interior Gateway Routing Protocol[2]

IGRP este un protocol dezvoltat de CISCO la mijlocul anilor '80. Multe dintre reţele au început să folosească acest protocol pentru că depăşeşte limitările la care erau supuse de către RIP. IGRP efectuează actualizarea tabelelor de rutare la fiecare 90 de secunde, fapt care conduce la o utilizare mai eficientă a lăţimii de bandă.

În calcularea rutelor disponibile, IGRP ia în calcul următorii factori:

- Lăţimea de bandă - administratorul poate configura lăţimea de bandă disponibilă pentru un segment de reţea sau o poate folosi pe cea implicită, care este specifică tipului legăturii existente.
- Întîrzierea - nu este calculată în mod dinamic. Se are în vedere suma întîrzierilor de pe fiecare interfaţa de ieşire din cadrul unei rute.
- Încrederea - este calculată dinamic în funcţie de posibilitatea transmiterii şi recepţionării pachetelor de tip keepalive. Trebuie configurată prin intermediul comenzii *metric weights*.
- Încărcătura - nu este folosită dacă nu este configurată comanda precedentă. În acest caz, gradul de încărcare al reţelei este calculat în mod dinamic.

1. Detalii la http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/rip.htm.
2. Detalii la http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/igrp.htm.

Spre deosebire de RIP, protocolul IGRP deţine un algoritm mai eficient prin care selectează ruta implicită. Cînd se foloseşte RIP, administratorul stabileşte o singură rută implicită, care este identificată ca fiind reţeaua 0.0.0.0.

IGRP-ul permite ca reţelele *reale* să fie marcate ca fiind candidate la rute implicite. Periodic, are loc o scanare a acestor rute candidate şi se alege cea care are cele mai bune valori ale unităţilor de măsură pentru a deveni rută implicită.

11.8. OSPF - Open Shortest Path First[1]

La începutul anilor '80, IETF recunoştea nevoia existenţei unui protocol de interior care să depăşească limitările impuse de RIP. Rezultatul muncii IETF s-a concretizat în apariţia OSPF.

Dintre avantajele acestui protocol de rutare amintim:

- Este un standard deschis acceptat de majoritatea producătorilor de echipamente;
- Convergenţa este mai rapidă decît la RIP;
- Oferă o securitate mai bună;
- Oferă suport pentru VLSM (variable-length subnet mask);
- Transmite cadre multicast în loc de broadcast;
- Nu consumă prea mult din lăţimea de bandă a reţelei.

Pentru a diminua utilizarea lăţimii de bandă, OSPF transmite în reţea doar schimbările intervenite în cadrul tabelelor de rutare. Traficul în reţea se limitează la sincronizarea bazelor de date, sincronizare ce apare la fiecare 30 de minute.

Routerele care rulează acest protocol acumulează informaţii cu privirea la starea legăturilor existente şi calculează cel mai scurt drum către o anumită reţea. Acest algoritm de calcul se numeşte SPF (*shortest path first*) sau Dijkstra. Rezultatul acestui calcul este o bază de date cu topologia cunoscută (*link state database*).

Din această bază de date, fiecare router construieşte un arbore cu cele mai scurte rute, arbore în care routerul care realizează acest calcul este rădăcina.

Vom dezvolta puţin reţeaua din capitolul 12 adăugînd cîteva dispozitive. Cum v-aţi obişnuit deja înainte, vom fac o scurtă trecere în revistă a comenzilor disponibile.

11.9. Comenzi IOS

Lucrul de la prompter este identic cu prezentarea făcută la switch-uri.

Comanda *enable* permite vizualizarea şi modificarea configuraţiei routerului în modul de lucru privilegiat:

```
Router>enable
```

1. Definit prin RFC 2178. Detalii la http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ospf.htm.

Părăsirea acestui mod de lucru se face cu ajutorul comenzii *disable*. Părăsirea consolei de lucru se face prin comanda *logout* sau *exit*. Ca şi în cazul switch-ului, configurarea routerului se face cu ajutorul comenzii *config*.

```
Router#config
Configuring from terminal, memory, or network [terminal]?
```

Pentru a modifica setările unei interfeţe se foloseşte comanda *interface*:

```
Router(config)#interface?
  Async                 Async interface
  BVI                   Bridge-Group Virtual Interface
  Dialer                Dialer interface
  Ethernet              IEEE 802.3
  Group-Async           Async Group interface
  Lex                   Lex interface
  Loopback              Loopback interface
  Null                  Null interface
  Port-channel          Ethernet Channel of interfaces
  Serial                Serial
  Tunnel                Tunnel interface
  Virtual-Template      Virtual Template interface
  Virtual-TokenRing     Virtual TokenRing
```

Unele router nu suportă interfeţe fast ethernet, caz în care în loc de comanda *interface fast Ethernet* trebuie să folosiţi *interface ethernet*:

```
Router(config)#interface ethernet 0
Router(config-if)#
```

Pe fiecare interfaţă a unui router se pot crea sub-interfeţe (interfeţe virtuale pentru situaţiile în care avem VLAN-uri). Dacă routerul suport este Fast Ethernet, comanda va *fi int f0/0.1*

```
Router(config-if)#interface ethernet 0.1
Router(config-subif)#
```

Nici în cazul routerului nu trebuie să trecem cu vederea partea de securitate. Pentru configurarea parolelor pentru modul de lucru utilizator se foloseşte comanda *line*:

```
Router(config)#line?
  <0-6>     First Line number
  aux       Auxiliary line
  console   Primary terminal line
  vty       Virtual terminal
```

Se pot activa două parole pentru modul de configurare global:

```
Router#config
```

```
Configuring from terminal, memory, or network [terminal]?t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#enable?
  last-resort  Define enable action if no TACACS servers
               respond
  password     Assign the privileged level password
  secret       Assign the privileged level secret
  use-tacacs   Use TACACS to check enable passwords
```

Pentru modul de lucru utilizator parola se va seta folosind comanda *line*:

```
Router(config)#line?
  <0-6>     First Line number
  aux       Auxiliary line
  console   Primary terminal line
  vty       Virtual terminal
```

- **aux** - se foloseşte pentru parola utilizator pentru portul auxiliar de configurare;
- **vty** – setează o parolă Telnet pentru conexiunea la router. Dacă nu se setează o astfel de parolă, telnetul nu poate fi folosit pentru conectarea la router;
- **console** – setează parola pentru configurarea routerului de la consolă.

Pentru configurarea parolei modului utilizator se alege linia dorită şi opţiunea *login* sau *no login*, prin care va spune routerului cum să se comporte la autentificare (cere sau nu parolă).

```
Router(config)#line aux 0
Router(config-line)#login
Router(config-line)#password ...... (parola)
```

Pentru a seta parola consolei folosiţi comanda *line console 0*.

```
Router(config)#line console?
  <0-0>   First Line number
Router(config)#line console 0
Router(config-line)#password.... (parola)
```

Am ales line 0, pentru că există doar un port pentru configurare de la consolă. Pentru configurarea consolei există cîteva comenzi opţionale care este bine să nu fie trecute cu vederea:

- *Exec-timeout 0 0* - intervalul de timp cît se poate lucra de la consolă;
- *Logging synchronous* - inhibă afişarea mesajelor pop-up ale consolei în timp ce lucraţi.

```
Router(config)#line con 0
Router(config-line)#exec-timeout?
  <0-35791>   Timeout in minutes
```

```
Router(config-line)#exec-timeout 0?
  <0-2147483>  Timeout in seconds
  <cr>
Router(config-line)#exec-timeout 0 0 (lucru fără timeout)
Router(config-line)#logging synchronous
```

Luînd în calcul toate lucrurile rele ce se pot întîmpla, vom seta şi o parolă pentru o sesiune Telnet. Se accesează modul de lucru utilizator cu ajutorul comenzii *line vty*. Pentru a vedea cîte linii suportă versiunea IOS de pe router, folosiţi *line vty 0*:

```
Router(config)#line vty 0?
  <1-4>  Last Line number
  <cr>
Router(config)#line vty 0 4
Router(config-line)#login
Router(config-line)#password.....
```

Dacă încercaţi să vă conectaţi prin Telnet la un router care nu are setată parolă pentru o astfel de conexiune, primiţi un mesaj de avertizare în acest sens. Se poate trece de acest neajuns folosind comanda *no login*, ceea ce va permite conexiune fără parole. Nu este însă sigur ! ! ! Parolele folosite pot fi criptate folosind *service password-encryption*:

```
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#service password-encryption
Router(config)#enable password adim
Router(config)#line vty 0 197
Router(config-line)#login
Router(config-line)#password adim1
Router(config-line)#line con 0
Router(config-line)#login
Router(config-line)#password adim2
Router(config-line)#line aux 0
Router(config-line)#login
Router(config-line)#password adim3
Router(config-line)#exit
Router(config)#no service password-encryption
Router(config)#^Z
%SYS-5-CONFIG_I: Configured from console by console
Router#sh run
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
```

```
!
hostname Router
!
!
enable password 7 7C4I0Y9F
!
ip subnet-zero
!
interface Ethernet0
 no ip address
 no ip directed-broadcast
 shutdown
!
interface Serial0
 no ip address
 no ip directed-broadcast
 shutdown
!
interface Serial1
 no ip address
 no ip directed-broadcast
 shutdown
line con 0
  password 7 7N9W4L5Z5D
  login
line aux 0
  password 7 7V7X8P9I0A
line vty 0 4
line vty 0 197
  password 7 6X5S2Y5Q5J
  login
```

Configurarea protocoalelor de rutare suportate de router se face folosind comanda *router <nume_protocol>* :

```
Router(config)#router rip
Router(config-router)#
```

Să presupunem că vrem să configurăm data şi ora de pe router:

```
Router#clock?
  set   Set the time and date
Router#clock set?
  hh:mm:ss  Current Time
Router#clock set 20:05:25 27 march 2003
```

```
Router#show clock
  20:05:25.526 UTC 25 July 2003
```

Comanda prin care se pot obține principalele informații despre un router este *show version*. Pentru a vizualiza informațiile despre configurația care rulează pe router se folosește *show running-config*, iar pentru a vedea configurația care se încarcă la pornirea sa, comanda este *show startup-config* :

```
Router#sh run
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
!
!
ip subnet-zero
!
interface Ethernet0
 no ip address
 no ip directed-broadcast
 shutdown
!
interface Serial0
 no ip address
 no ip directed-broadcast
 shutdown
!
interface Serial1
 no ip address
 no ip directed-broadcast
```

Configurația cu care startează routerul poate fi ștearsă cu ajutorul comenzii *erase startup-config* :

```
Router#erase startup-config
Erasing the nvram filesystem will remove all files! Continue? [confirm]
```

Configurația introdusă de la prompt se salvează în NVRAM folosind comanda *copy running-config, startup-config* sau *copy run start* (la versiunile mai noi de IOS). Dacă sesiunile de lucru nu se finalizează cu această comandă sau o alta care permite salvarea, ați muncit degeaba!

Router#copy run start - în acest moment fişierul de configurare creat va fi plasat în NVRAM de unde va fi folosit la următoarea bootare a routerului.

Ca şi în cazul switch-urilor, interfeţele unui router se configurează din modul global:

```
Router(config)#interface?
  Async                    Async interface
  BVI                      Bridge-Group Virtual Interface
  Dialer                   Dialer interface
  Ethernet                 IEEE 802.3
  Group-Async              Async Group interface
  Lex                      Lex interface
  Loopback                 Loopback interface
  Null                     Null interface
  Port-channel             Ethernet Channel of interfaces
  Serial                   Serial
  Tunnel                   Tunnel interface
  Virtual-Template         Virtual Template interface
  Virtual-TokenRing        Virtual TokenRing
Router(config)#interface
```

Observaţi că, spre deosebire de switch-uri, routerul are mai multe tipuri de interfeţe. În acest moment, pe noi ne interesează doar cele seriale[1] şi ethernet.

```
Router(config)#interface serial?
  <0-1> Serial interface number
```

Comanda de mai sus indică faptul că acest model de router are două interfeţe seriale.

```
Router(config)#interface Ethernet?
  <0-0>  Ethernet interface number
```

Comanda de mai sus indică faptul că routerul folosit are o singură interfaţă Ethernet. Se cuvine să facem o precizare legată de notaţia interfeţelor. În cazul routerelor mici (seriile mici), numărul interfeţei este format dintr-o singură cifră. La modelele mai complexe, numărul interfeţei este alcătuit din numărul slotului în care este montată cartela, un slash urmat apoi de numărul portului de pe cartelă[2].

Pentru routerele care suportă şi sloturi, comanda de configurare a interfeţei este similară cu cea a switch-urilor: *interface <tip interfaţă> <număr slot/port>*. După configurare, interfeţele trebuie activate pentru a deveni operaţionale. Activarea/dezactivarea unei interfeţe se face cu ajutorul comenzilor *shutdown/no shutdown*. Dacă o interfaţă este dezactivată, acest lucru va fi afişat dacă folosiţi comanda *show interface*. La pornirea unui router, interfeţele sînt implicit dezactivate.

---

1. Interfeţele seriale sînt folosite pentru a conecta routerele între ele pe distanţe scurte.
2. De exemplu, portul Ethernet 3 de pe cartela montată în slotul doi va fi numerotat E2/3. Pentru detalii legate de interfeţele fiecărui model de router, vizitaţi *www.cisco.com/univercd/cc/td/doc/pcat*.

```
Router#sh int e0
Ethernet0 is administratively down, line protocol is down
   Hardware is Lance, address is 0010.7b81.65e9(bia 0010.
   7b81.65e9)
   Description:
   Internet address is 0.0.0.0
   MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 252/
   255, load 1/255
   Encapsulation ARPA, loopback not set, keepalive set (10 sec)
   ARP type: ARPA, ARP Timeout 04:00:00
   Last input never, output 02:11:34, output hang never
   Last clearing of "show interface" counters never
   Queueing strategy: fifo
   Output queue 0/40, 0 drops; input queue 0/75, 0 drops
   5 minute input rate 0 bits/sec, 0 packets/sec
   5 minute output rate 0 bits/sec, 0 packets/sec
      0 packets input, 0 bytes, 0 no buffer
      Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
```

Activarea interfeţei :

```
Router(config)#int e0
Router(config-if)#no shutdown
%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0,
changed state to up
%LINK-3-UPDOWN:  Interface Ethernet0, changed state to up
Router(config-if)#exit
Router(config)#exit
Router#sh int e0
Ethernet0 is up, line protocol is up
   Hardware is Lance, address is 0010.7b81.65e9(bia 0010.
   7b81.65e9)
   Description:
   Internet address is 0.0.0.0
   MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 252/
   255, load 1/255
   Encapsulation ARPA, loopback not set, keepalive set (10 sec)
   ARP type: ARPA, ARP Timeout 04:00:00
   Last input never, output 02:11:34, output hang never
   Last clearing of "show interface" counters never
   Queueing strategy: fifo
   Output queue 0/40, 0 drops; input queue 0/75, 0 drop
   5 minute input rate 0 bits/sec, 0 packets/sec
   5 minute output rate 0 bits/sec, 0 packets/sec
      0 packets input, 0 bytes, 0 no buffer
      Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
```

Nu uitaţi deci să activaţi fiecare interfaţă care doriţi să fie activă pe routerul administrat. Să luăm ca exemplu o interfaţă cu adresa 172.16.10.1/24:

```
Router(config)#int e0
Router(config-if)#ip address 172.16.10.2 255.255.255.0
Router(config-if)#no shut
```

Spuneam mai devreme că routerul are şi interfeţe seriale. Pentru aceste interfeţe trebuie configurată conexiunea DCE (am menţionat deja ce înseamnă acest lucru):

```
Router(config)# int s0
Router(config-if)#clock rate?
Speed(bits per second)
  1200
  2400
  4800
  9600
  19200
  38400
  56000
  64000
  72000
  125000
  148000
  250000
  500000
  800000
  1000000
  1300000
  2000000
  4000000
  <300-8000000>    Choose clockrate from list above
```

Dacă interfaţa respectivă nu are conexiune la DCE, veţi obţine un mesaj de eroare. De ce trebuie configurate totuşi aceste interfeţe (lăţimea de bandă)? Lăţimea de bandă de pe intefeţele seriale este folosită de către protocoalele de rutare (IGRP, EIGRP, OSPF) pentru a calcula cel mai bun transport către un host din reţea. În cazul protocolului RIP (mai bătrîn), lăţimea de bandă a unei astfel de interfeţe nu prezintă importanţă.

```
Router(config-if)#bandwidth?
  <1-10000000>  Bandwidth in kilobits
Router(config-if)#bandwidth 64
```

11.10. Studiu de caz

Din vechea diagramă mai trebuie configurată rutarea între serverele din cele două VLAN-uri. Dar pînă acolo trebuie să vedem de ce mai este nevoie.

Router A şi router B sînt conectate între ele printr-o legătură serială. Sw_Stud4 se conectează la Router B prin interfața Fast Ethernet 0/26, iar conectarea serverului studenți se face prin interfața Ethernet 0/1. Acest server face parte din rețeaua 172.16.20.0/24.

Pornim la lucru începînd cu Router A cu mențiunea că se conectează la două rețele: 172.16.10.0/24 (din exemplul precedent) şi 172.16.20.0/24.

Mai întîi, vom configura parolele de acces şi interfețele.

```
Router>enable
Router#config t
Router(config)#hostname Router_A
Router_A(config)#enable secret adim
Router_A(config)#line console 0
Router_A(config-line)#login
Router_A(config-line)#password adim
Router_A(config-line)#line aux 0
Router_A(config-line)#login
Router_A(config-line)#password adim
Router_A(config-line)#line vty 0 4
Router_A(config-line)#login
Router_A(config-line)#password adim
Router_A(config-line)#interface ethernet0
Router_A(config-if)#ip address 172.16.10.1 255.255.255.0
Router_A(config-if)#description Conectare la reteaua 10
Router_A(config-if)#no shutdown
Router_A(config-if)#interface serial0
Router_A(config-if)#ip address 172.16.20.1 255.255.255.0
Router_A(config-if)#description Conectare la routerul Router_B
Router_A(config-if)#no shutdown
Router_A(config-if)#exit
```

Routerul A este conectat la rețelele 172.16.10.0 şi 172.16.20.0. Pentru fiecare dintre rețelele care nu sînt conectate direct la acest router ar trebui configurată o rută.

Observați din schemă că următorul *hop* va fi întotdeauna 172.16.20.1, adică routerul B. Pentru a configura rutele *statice* se va folosi comanda *ip route*.

```
Router_A(config)#ip route 172.16.10.0 255.255.255.0
172.16.20.1
```

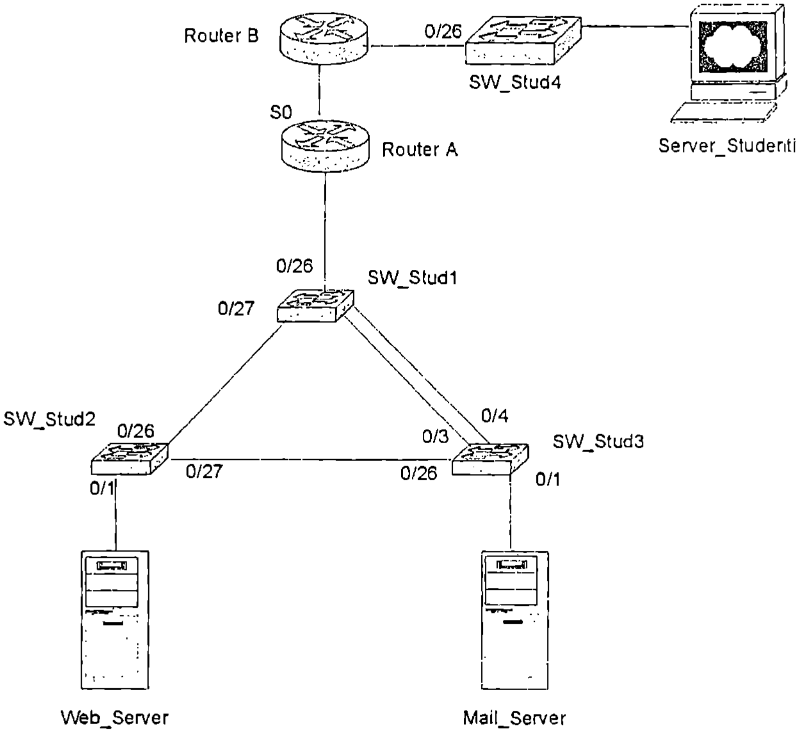


Figura 11.10.1. Diagramă de rețea

Pentru a vizualiza rutele introduse se apelează comanda *show ip route*:

```
Router_A#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M -
mobile, B -  BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
       inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA
       external type 2
       E1 - OSPF external type 1, E2 - OSPF external type
       2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       * - candidate default
       U - per-user static route, o - ODR

Gateway of last resort is not set

         172.16.0.0/24 is subnetted, 2 subnets
```

```
C          172.16.20.0 is directly connected. Serial0
S          172.16.10.0 [1/0] via 172.16.20.1.
C          172.16.10.0 is directly connected. Ethernet0
```

Dacă reţeaua este mare, varianta rutelor statice nu mai reprezintă soluţia optimă. Se apelează la varianta rutelor implicite (*default*). *Default route* diferă de configurarea default gateway-ul de pe o staţie, deoarece routerul însuşi este un gateway. Ceea ce poate fi configurat în acest caz pe un router se numeşte *Gateway of Last Resort*, ceea ce înseamnă că dacă un pachet are ca destinaţie o reţea care nu apare în tabela de rutare, va fi transmis către o destinaţie implicită.

După cum se vede din schemă, routerele noastre primesc informaţii dintr-o reţea şi trebuie să le transmită către o alta. Este o situaţie tipică de configurare a unor astfel de rute. Pentru aceasta, mai întîi trebuie şterse rutele introduse (*no ip route*). Pentru Router_A ruta implicită (default) este către Router_B:

```
Router_A(config)#no ip route 172.16.10.0 255.255.255.0
172.16.20.1
Router_A(config)#exit
Router_A#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M -
       mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
       inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA
       external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2,
       E - GP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       * - candidate default
       U - per-user static route, o - ODR

Gateway of last resort is not set

           172.16.0.0/24 is subnetted, 2 subnets
C          172.16.20.0 is directly connected. Serial0
C          172.16.10.0 is directly connected. Ethernet0

Router_A(config)#ip route 0.0.0.0 0.0.0.0 172.16.20.1
Router_A(config)#ip classless
Router_A(config)#exit
Router_A#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M -
       mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
       inter area
```

```
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA
       external type 2
       E1 - OSPF external type 1, E2 - OSPF external type
       2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       * - candidate default
       U - per-user static route, o - ODR

Gateway of last resort is 172.16.20.1 to network 0.0.0.0

         172.16.0.0/24 is subnetted, 2 subnets
C        172.16.20.0 is directly connected. Serial0
C        172.16.10.0 is directly connected. Ethernet0
S*       0.0.0.0 [1/0] via 172.16.20.1
Router_A#
```

În comanda *ip route* am folosit numai zero pentru numărul rețelei și subnet mask pentru a scoate în evidență că este vorba de toate rețelele și toate subnet mask-urile. Comanda *ip classless* spune routerului să nu distrugă pachetele recepționate, ci să le transmită către ruta implicită.

Vom configura acum rutarea dinamică cu ajutorul protocoalelor pentru rutare. Pentru început vom apela la RIP, nu înainte de a șterge rutele implicite create anterior:

```
Router_A(config)#no ip route 0.0.0.0 0.0.0.0 172.16.20.1
Router_A(config)# router rip
Router_A(config-router)#network 172.16.0.0
```

Dacă se dorește configurarea IGRP (situația în care rețeaua este mai complexă), se procedează aproape similar, cu mențiunea că routerele trebuie să facă parte din cadrul aceluiași sistem autonom (în cazul nostru vom folosi 10). Mai întîi trebuie să ștergeți routarea cu RIP (*no router rip*):

```
Router_A(config)#router igrp 10
Router_A(config-router)#network 172.16.0.0
Router_A(config-router)#exit
```

Ne mutăm la routerul B din schema noastră. Multe dintre configurări sînt identice. Diferența apare în cazul interfeței seriale unde trebuie configurată conexiunea DCE:

```
Router>enable
Router#config t
Router(config)#hostname Router_B
Router_B(config)#enable secret adim
Router_B(config)#line console 0
Router_B(config-line)#login
Router_B(config-line)#password adim
```

```
Router_B(config-line)#line aux 0
Router_B(config-line)#login
Router_B(config-line)#password adim
Router_B(config-line)#line vty 0 4
Router_B(config-line)#login
Router_B(config-line)#password adim
Router_B(config-line)#interface ethernet0
Router_B(config-if)#ip address 172.16.30.1 255.255.255.0
Router_B(config-if)#description Conectare la reteaua 30
Router_B(config-if)#no shutdown
Router_B(config-if)#interface serial0
Router_B(config-if)#ip address 172.16.20.2 255.255.255.0
Router_B(config-if)#description  Conectare  la  routerul
Router_A
Router_B(config-if)#no shutdown
Router_B(config-if)#clock rate 64000
Router_B(config-if)#exit
Router_B(config)#router igrp 10
Router_B(config-router)#network 172.16.0.0
```

Vom vizualiza rutele și protocoalele care rulează pe cele două routere. Pentru routerul B :

```
Router_B#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M -
       mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
       inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA
       external type 2
       E1 - OSPF external type 1, E2 - OSPF external type
       2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       * - candidate default
       U - per-user static route, o - ODR

Gateway of last resort is not set

           172.16.0.0/24 is subnetted, 3 subnets
C          172.16.30.0 is directly connected. Ethernet0
C          172.16.20.0 is directly connected. Serial0
I          172.16.10.0 [100/1] via 172.16.20.1.
           00:00:18. Serial0

Router_B#sh ip protocols
Routing Protocol is "igrp 10"
```

```
  Sending updates every 90 seconds, next due in 37 seconds
  Invalid after 270 seconds, hold down 280, flushed after 630
  Outgoing update filter list for all interfaces is
  Incoming update filter list for all interfaces is
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  IGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  IGRP maximum hopcount 100
  IGRP maximum metric variance 1
  Redistributing: igrp 10
  Default version control: send version 1, receive any
  version
    Interface          Send    Recv    Key-chain
    Ethernet0          1       1 2
    Serial0            1       1 2
  Routing for Networks:
    172.16.0.0
  Routing Information Sources:
    Gateway           Distance        Last Update
    172.16.20.1            100        00:00:21
    Distance:(default is 100)
```

Pentru routerul A:

```
Router_A#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M -
       mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
       inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA
       external type 2
       E1 - OSPF external type 1, E2 - OSPF external type
       2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       * - candidate default
       U - per-user static route, o - ODR

Gateway of last resort is not set

         172.16.0.0/24 is subnetted, 3 subnets
I        172.16.30.0 [100/1] via 172.16.20.2.
         00:00:18. Serial0
C        172.16.20.0 is directly connected. Serial0
C        172.16.10.0 is directly connected. Ethernet0
Router_A#sh ip protocols
```

```
Routing Protocol is "igrp 10"
  Sending updates every 90 seconds, next due in 37 seconds
  Invalid after 270 seconds, hold down 280, flushed after 630
  Outgoing update filter list for all interfaces is
  Incoming update filter list for all interfaces is
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  IGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  IGRP maximum hopcount 100
  IGRP maximum metric variance 1
  Redistributing: igrp 10
  Default version control: send version 1, receive any version
    Interface        Send   Recv   Key-chain
    Ethernet0        1      1 2
    Serial0          1      1 2
  Routing for Networks:
    172.16.0.0
  Routing Information Sources:
    Gateway          Distance        Last Update
    172.16.20.2           100        00:00:21
    Distance:(default is 100)
```

Ce ar mai fi de făcut? Destul de multe. Nu ne-am propus să le rezolvăm chiar pe toate, aşa că vom mai trata doar două subiecte: cum se pot crea tabele cu host-uri pe un router şi listele pentru controlul accesului.

Aţi observat că, în practică, de multe ori folosiţi numele calculatorului, şi nu adresa sa IP. Este mult mai comod. Acelaşi lucru este valabil şi în cazul routerelor. Acestea trebuie însă să fie capabile să transforme numele dispozitivului într-o adresă IP.

O tabelă cu host-uri rezolvă această problemă doar pe routerul pe care a fost creată! Vom exemplifica o astfel de situaţie pentru routerul B şi switch-ul SW_Stud4: cum putem rezolva aceste nume de pe Router A. Comanda folosită este *ip host <nume adresă ip>* :

```
Router_A(config)#ip host router_B?
  <0-65535>   Default telnet port number
  A.B.C.D     Host IP address(maximum of 8)

Router_A(config)#ip host router_B 172.16.20.2
Router_A(config)#ip host SW_Stud4 172.16.30.2
Router_A(config)#exit
Router_A#sh host
Default domain is not set
Name/address lookup uses domain service
Name servers are 255.255.255.255

Host                  Flags        Age  Type   Address(es)
```

```
sw stud4            (perm, OK) 0    IP     172.16.30.2
router b            (perm, OK) 0    IP     172.16.20.2
```

În acest moment ne putem conecta de pe routerul A pe B doar tastînd numele routerului la prompt (acum vă daţi seama de ce este bine să avem parole setate pentru fiecare tip de conexiune):

```
Router_A#router_b
Trying 172.16.20.2 ... Open

Router_A#SW_Stud4
Trying 172.16.30.2 ...

Catalyst 1900 Management Console
Copyright (c) Cisco Systems, Inc.  1993-1999
All rights reserved.
Enterprise Edition Software
Ethernet Address:        00-30-80-C7-BE-C0

PCA Number:              73-3122-04
PCA Serial Number:       FAB033723WJ
Model Number:            WS-C1912-A
System Serial Number:    FAB0338S10A
Power Supply S/N:        APQ032404SA
PCB Serial Number:       FAB033723WJ,73-3122-04
------------------------------------------------

1 user(s) now active on Management Console.

        User Interface Menu

     [M] Menus
     [K] Command Line

Enter Selection:
Enter password:
```

Dacă doriţi să renunţaţi la tabele, folosiţi comanda *no ip host*.

O problemă spinoasă cu care se confruntă administratorii de reţea o reprezintă traficul mai puţin dorit în reţeaua lor.

Routerele oferă facilităţi de filtrare a traficului prin intermediul *listelor pentru controlul accesului (Access Control Lists - ACL[1])*. Aceste liste nu reprezintă altceva decît

1. Pentru mai multe detalii vizitaţi http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/secur_c/scprt3/scacls.htm.

un set de instrucțiuni secvențiale care se aplică interfețelor routerului. Instrucțiunile respective indică routerului care sînt pachetele pe care trebuie să le accepte și pe care nu. Cum subiectul este destul de vast, în rîndurile următoare vă vom oferi doar elementele care să vă orienteze în continuare.

Ca regulă generală, ACL-urile se creează pentru fiecare protocol care se dorește a fi filtrat prin intermediul routerului: se specifică protocolul, se asociază un număr de identificare a listei și se definesc criteriile care se aplică în filtrarea pachetelor.

Intervalul 1-99 identifică listele standard, iar intervalul 100-199 listele extinse. ACL-urile standard sînt cele care verifică adresa sursă a pachetului (motiv pentru care trebuie create pe routerul cel mai apropiat de rețeaua destinație) în timp ce ACL-urile extinse verifică atît adresa sursă, cît și pe cea destinație.

În exemplul nostru, vom bloca accesul serverului Studenți în rețeaua 172.16.10.0, dar vom permite accesul către această rețea oricărui alt calculator. Pentru aceasta, ne vom conecta la routerul cel mai apropiat de rețeaua destinatară, Router_A, pe care vom crea o listă standard:

```
Router_A(config)#access-list 10 deny host 172.16.30.10
Router_A(config)#access-list 10 permit any
```

Lista astfel creată trebuie asociată unei interfețe. În cazul nostru este vorba de interfața serială S0:

```
Router_A(config)#interface serial 0
Router_A(config-if)#ip access-group 10 in
```

În acest moment, dacă vom folosi comanda ping pe serverul Studenți, vom observa că nici unul dintre celelalte servere nu mai răspunde.

Să presupunem acum că dorim să blocăm accesul la serverul de mail (telnet) din rețeaua 172.16.30.0. Pentru aceasta, pe același router vom crea o listă extinsă, după ce în prealabil ștergem lista creată anterior:

```
Router_A(config)#no access-list 10
Router_A(config)#interface serial 0/0
Router_A(config-if)#no ip access-group 10 in

Router_A(config)#access-list 101 deny tcp host 172.16.30.10
172.16.10.0 0.0.0.255 eq telnet
Router_A(config)#access-list 101 permit ip any any
Router_A(config)#int fast 0/0
Router_A(config-if)#ip access-group 101 out
```

Pentru detalii privind acest subiect nu ezitați să vizitați http://www.cisco.com/univercd/cc/td/doc/product/software/ios113cd/113cd_cr/secur_c/scprt3/scacls.htm#xtocid2689513.

CAPITOLUL 12

Proiectarea şi administrarea reţelelor

Proiectarea reţelelor înseamnă întotdeauna mai mult decît conectarea a două sau mai multe calculatoare între ele. Prima etapă a oricărui astfel de proiect[1] constă în stabilirea unor obiective, specifice fiecărei organizaţii în parte. Chiar dacă avem în vedere specificul firmei, cînd proiectăm o reţea, trebuie să ţinem cont de :

- **Funcţionalitate** : reţeaua trebuie să funcţioneze optim.
- **Scalabilitate** : reţeaua trebuie să ofere posibilităţi de dezvoltare ulterioară.
- **Adaptabilitate** : reţeaua trebuie dezvoltată astfel încît să nu includă elemente care îi vor restricţiona dezvoltările ulterioare.
- **Gestionare** : reţeaua trebuie dezvoltată astfel încît să permită monitorizarea.

În funcţie de situaţia de pe teren există două cazuri : proiectare şi reproiectare. Cea de a doua variantă este de cele mai multe ori şi cea mai dificilă. Ne propunem în cele ce urmează doar o scurtă iniţiere în ceea ce înseamnă un proiect de reţea, din mai multe motive.

În primul rînd, trebuie să ţinem cont de punctul de vedere al utilizatorilor care îşi doresc o reţea fără întîrzieri, fără constrîngeri legate de protocoale sau medii de transmisie, fără erori, cît mai portabilă şi uşor de utilizat. În realitate însă proiectantul se loveşte de limitările tehnologiilor existente, de bugetul de care dispune firma, de aplicaţiile care rulează în firmă etc.

12.1. Proiectarea structurată a unei reţele de calculatoare[2]

Literatura de specialitate[3] recomandă un model ierarhic pe trei niveluri în baza căruia să fie proiectate topologiile reţelelor. Acesta este modelul tradiţional folosit în proiectarea reţelelor :

- Nivelul central (*Core*) ;

1. Vezi şi Oprea D., *Managementul proiectelor. Teorie şi cazuri practice*, Ed. Sedcom Libris, Iaşi, 2001
2. Detalii privind particularităţile proiectării la adresa *http://www.cisco.com/univercd/cc/td/doc/cisintwk/idg4/index.htm*.
3. Ne referim mai ales la publicaţiile Cisco Systems Inc, Bay Networks, Nortell. Pot fi luate în calcul şi modele care au în vedere în primul rînd securitatea reţelei.

- Nivelul distribuție (*Distribution*) ;
- Nivelul acces (*Access*).

Nivelul central reprezintă coloana vertebrală a viitoarei rețele (backbone-ul). După cum îi spune și numele, trebuie să fie nivelul cu capacitatea cea mai rapidă de adaptare la schimbări și să dețină componente redundante. Viteza de comutare a pachetelor este critică : pe routerele instalate la acest nivel nu se vor efectua filtrări de pachete. Latența trebuie să fie cît mai mică.

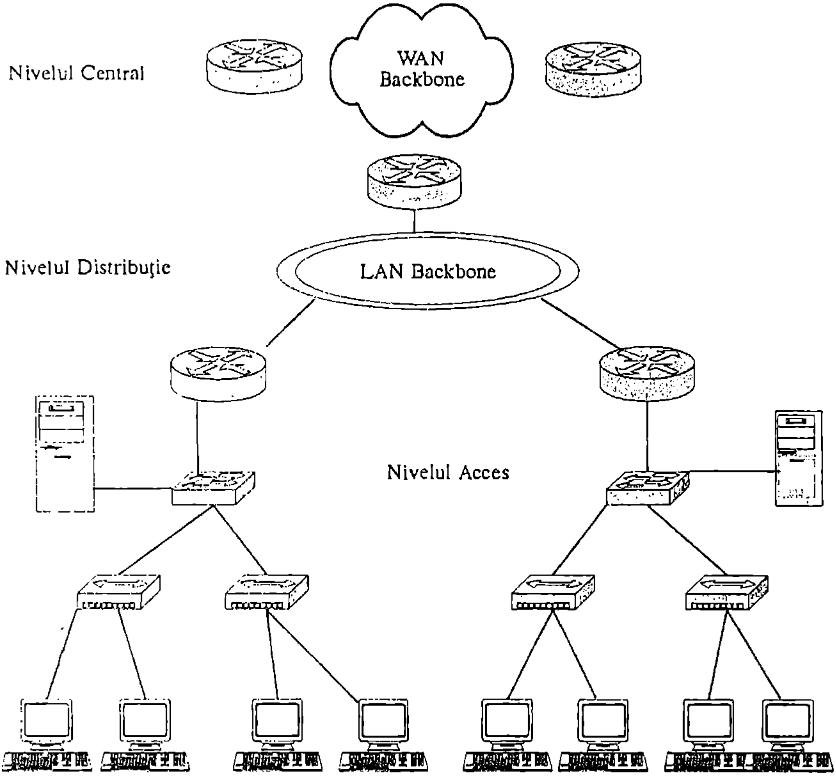


Figura 12.1.1. Modelul ierarhic de proiectare a unei rețele
(Sursa : *http : //www.cisco.com/univercd/cc/td/doc/ cisintwk/idg4/index.htm*)

Pentru firmele care doresc conexiuni la filiale prin intermediul extra sau Internetului, acest nivel trebuie să includă, în mod obligatoriu, una sau mai multe legături spre exterior. Administratorii de la nivel central trebuie să descurajeze realizarea în filiale a propriilor conexiuni (este softul celor de la Cisco). Motivul? Centralizarea acestor funcții reduce problemele legate de rutare și securitate.

Nivelul distribuţie are rolul de a controla accesul la resurse (securitatea reţelei), traficul reţelei şi domeniile de broadcast. În cazul în care se apelează la soluţia VLAN-urilor, acest nivel va realiza rutarea între reţelele virtuale.

Pentru a creşte performanţele protocoalelor pentru rutare, pe routerele din cadrul acestui nivel pot fi introduse rutele de la nivelul acces sau, dacă este nevoie, rutele implicite către nivelul acces.

Tot acest nivel poate să ofere suport pentru NAT (*network address translation*), astfel încît dispozitivile de la nivelul acces să poată folosi adrese IP private.

Nivelul acces este cel care oferă utilizatorilor acces la segmentul local al reţelei. Este posibil să fie incluse routere chiar şi la acest nivel.

Pînă acum cîţiva ani, cînd se punea problema proiectării unei reţele, se spunea că trebuie respectată regula 80-20: 80% din traficul unei reţele este intern şi doar 20% trebuie rutat către exterior. Astăzi, această regulă nu mai este respectată, în principal datorită aplicaţiilor folosite în firme.

Caracterizarea reţelei existente

Nu putem proiecta o reţea fără a şti care este situaţia de fapt de pe teren. Altfel spus, proiectarea unei reţele trebuie să respecte principiile generale ale proiectării structurate. Prin urmare, începutul este dat de etapa de analiză! Ce aspecte interesează? La această întrebare vom răspunde în continuare. Un proiect de reţea are la bază cerinţele utilizatorilor şi tehnologiile existente la un moment dat. Nu avem pretenţia că cele prezentate în continuare acoperă toate aspectele ce interesează într-un astfel de proiect. Lista reprezintă doar un punct de plecare ce poate fi dezvoltat în funcţie de caracteristicile şi obiectivele firmei.

1. *Identificarea aplicaţiilor care rulează în reţea*

Reţeaua va fi cea care va oferi suport pentru aplicaţiile utilizatorilor, şi nu invers. Acest lucru înseamnă că toate aplicaţiile care rulează sau vor rula în firmă trebuie să fie documentate. Fiecare aplicaţie are propriile sale cerinţe legate de trafic şi circuitul informaţiilor. Este primul şi cel mai important pas în proiectarea unei reţele.

Tabelul 12.1.1. Inventarul aplicaţiilor care rulează în reţea

Denumirea aplicaţiei	Tipul	Numărul de utilizatori	Numărul de servere/host-uri	Segmentul de reţea	Comentarii
Se completează cu denumirea fiecărei aplicaţii care rulează în reţea	Se precizează dacă este vorba de o bază de date, aplicaţie pentru grupuri de lucru, intranet etc.	Numărul de utilizatori care lucrează cu respectiva aplicaţie	Numărul de servere pe care rulează aplicaţia şi host-urile care o accesează	Pe care segment de reţea rulează aplicaţia respectivă	

Informaţiile culese în această fază vă ajută să înţelegeţi viitorul trafic al reţelei. Dacă ştiţi care este echipamentul sursă şi destinaţie, veţi identifica şi modul cum circulă

informaţiile între acestea (spre exemplu, dacă este vorba de un client şi un server Web, trebuie să aveţi în vedere şi protocolul folosit).

2. *Protocoalele care rulează în reţea*

După cum spuneam şi mai sus, o dată cu identificarea aplicaţiilor trebuie să avem în vedere şi protocoalele care sprijină acele aplicaţii.

Tabelul 12.1.2. Inventarul protocoalelor care rulează în reţea

Protocolul	Tipul protocolului	Numărul de utilizatori	Numărul de servere/host-uri	Comentarii
Se completează cu denumirea fiecărui protocol care rulează în reţea	Se precizează dacă este vorba de un protocol rutabil, nerutabil, pentru rutare etc.	Numărul de utilizatori care lucrează cu respectivul protocol	Numărul de servere şi host-uri care rulează protocolul	

3. *Documentarea reţelei*

În această etapă trebuie obţinute informaţii cît mai detaliate despre topologia reţelei şi schema de adresare folosită.

Existenţa unei documentaţii a reţelei (chiar şi o schemă) este punctul de pornire pentru viitorul proiect. În lipsa unui astfel de instrument nu vă rămîne decît să creaţi o hartă a actualei reţele şi să o documentaţi. Schema reţelei trebuie să includă atît componenta logică (cum sînt conectate dispozitivele între ele), cît şi pe cea fizică (descrierea dispozitivelor, adresele folosite etc.). Cînd dezvoltaţi o astfel de schemă, ţineţi cont de următoarele aspecte:

- Trebuie reprezentate toate segmentele reţelei, chiar şi cele mai simple.
- Toate segmentele de reţea trebuie să aibă asociată o topologie şi o tehnologie.
- Schema de adresare folosită, maniera de alocare a adreselor (static, dinamic, NAT).

4. *Identificarea constrîngerilor proiectului*

Pentru a asigura reuşita proiectului este nevoie să înţelegem obiectivele firmei. Cisco[1] pune la dispoziţia proiectanţilor o listă de control pentru a verifica dacă s-au obţinut toate informaţiile prin care pot fi identificate constrîngerile firmei:

- Structura organizatorică a firmei.
- Circuitul informaţiilor.
- Datele şi activităţile considerate critice.
- Politicile cu privire la furnizorii de soluţii hard şi soft.
- Distribuirea autorizaţiilor cu privire la achiziţionarea/implementarea soluţiilor.
- Experienţa clientului.
- Politicile firmei care pot afecta proiectul.

1. CCDA Exam Certification Guide.

5. *Caracteristicile actuale ale reţelei*

O caracteristică importantă a reţelei o reprezintă timpul cît aceasta nu este funcţionabilă. Să ne gîndim ce ar însemna acest lucru pentru o agenţie de ştiri? Prin urmare, culegerea de date statistice despre modul de funcţionare a reţelei este un mijloc prin care puteţi caracteriza situaţia actuală:

- Ce segmente de reţea sînt considerate critice?
- Care este timpul mediu de nefuncţionare a reţelei într-o zi/lună?
- Care sînt motivele nefuncţionării?
- Care sînt pierderile datorate nefuncţionării?

Răspunzînd la aceste întrebări vom putea identifica mai uşor cerinţele legate de redundanţa unor segmente de reţea şi de costurile implicate. De asemenea, trebuie să avem în vedere performanţele: timpul de răspuns între două calculatoare, dispozitive sau aplicaţii. Ne interesează acest aspect pentru a putea compara timpii de răspuns actuali cu cei obţinuţi după reproiectare.

Tot în această fază, ne interesează gradul de utilizare a reţelei şi siguranţa acesteia. Pentru aceasta este nevoie de înţelegerea cît mai exactă a traficului pentru a capta şi analiza date relevante. Este una dintre etapele consumatoare de timp, deoarece documentarea şi înţelegerea traficului fiecărui segment de reţea, fără a afecta productivitatea acesteia, poate să dureze. Pe de altă parte, trebuie să faceţi apel la aplicaţii specializate de genul analizoarelor de trafic sau pentru protocoale. Informaţiile culese vizează:

- Numărul total de MB transmişi pe un segment.
- Numărul de cadre.
- Numărul de erori.
- Numărul de coliziuni apărute.
- Numărul de cadre broadcast sau multicast.

Pentru a caracteriza gradul de siguranţă a traficului reţelei, CISCO recomandă documentarea aspectelor menţionate anterior.

Trebuie să mai verificaţi:

1. dacă există segmente Ethernet saturate de trafic (maxim 40% utilizare);
2. dacă pe un segment există mai mult de 20% trafic broadcast sau multicast;
3. pe un segment să nu existe mai mult de o eroare CRC la un milion de bytes;
4. pe un segment să nu existe mai mult de 0,1% pachete în coliziune.

Analiza cerinţelor[1]

În acest moment, ar trebui să ştim care este situaţia de pe teren şi să putem decide care sînt noile cerinţe legate de proiectare. Pentru aceasta vom face apel tot la CISCO, care ne pune la dispoziţie o listă de control cu paşii care trebuie urmaţi pentru a organiza cît mai bine proiectul.

1. Vezi şi P. Oppenheimer, *Top-Down Network Design*, Cisco Press, 1999.

1. *Constrîngeri de natură economică*

Ne referim aici în primul rînd la înţelegerea mediului în care îşi desfăşoară firma activitatea şi la bugetul alocat unui astfel de proiect. Pentru ca proiectul să aibă succes, sînt necesare discuţii cu persoana care controlează bugetul.

Trebuie identificate cu exactitate resursele disponibile, gradul de instruire a utilizatorilor şi data la care reţeaua trebuie dată în folosinţă.

2. *Cerinţe legate de securitate*

Dacă proiectarea are la bază un model structurat, trebuie precizat gradul de securitate dorit în reţea şi maniera de implementare a politicilor de securitate : firewall, liste pentru controlul accesului etc.[1]. Trebuie avut în vedere modul în care se vor realiza autentificarea utilizatorilor şi drepturile de acces ale acestora. Acest lucru presupune cunoaşterea exactă a resurselor sistemului şi a manierei de utilizare a acestora (cine, ce, cînd, cum).

3. *Cerinţe legate de administrare*

Un prim aspect ce interesează îl reprezintă toleranţa la căderi. În caz de nefuncţionare a reţelei, administratorul este principalul răspunzător. El trebuie să poată administra cît mai bine configuraţiile echipamentelor care funcţionează în reţea precum şi performanţele dorite. Administratorul trebuie să fie capabil să identifice, să izoleze şi să corecteze problemele într-un timp cît mai scurt.

Aspectul cel mai important legat de administrare se referă la scalabilitatea[2] reţelei. Din acest punct de vedere, administratorul este interesat de următoarele aspecte :

- Numărul de servere şi staţii ce vor fi adăugate în reţea.
- Numărul de utilizatori care vor folosi resursele reţelei.
- Numărul de segmente independente de reţea ce vor trebui interconectate.

Această prognoză trebuie să acopere o perioadă de minimum 2 ani.

4. *Cerinţe legate de aplicaţii*

Aplicaţiile specifice utilizatorilor care vor rula în reţea trebuie identificate şi clasificate după cum urmează :

- Poştă electronică ;
- Acces la fişiere şi imprimante ;
- Aplicaţii pentru grupuri de lucru ;
- Transfer de fişiere ;
- Acces la baze de date ;
- Videoconferinţe ;
- Comerţ electronic ;
- Proiectare asistată de calculator ;
- ERP ;
- Controlul proceselor tehnologice etc.

---

1. Aşa, după cum există certificate în domeniul reţelelor, bazelor de date sau programării, pentru cei care doresc să se specializeze pe partea de securitate a unui sistem se poate obţine o certificare internaţională : CISSP (Computer Information System Security Professional). Vezi şi www.cissp.com.
2. Scalabilitatea se referă la capacitatea de dezvoltare a reţelei fără a fi nevoie de reproiectarea acesteia.

Trebuie avute în vedere şi aplicaţiile denumite *de sistem* :

- Autentificarea utilizatorilor ;
- Instalarea şi configurarea staţiilor de lucru de la distanţă ;
- Realizarea copiilor de siguranţă în reţea ;
- Distribuţia de software ;
- Managementul reţelei.

5. *Cerinţe legate de trafic şi performanţe*

De multe ori, cînd se proiectează o reţea, nu există specificaţii cu privire la performanţele pe care trebuie să le atingă reţeaua după ce aceasta devine funcţională. Dacă utilizatorii îşi pot desfăşura activitatea, totul este în regulă. Pe de altă parte, există situaţii în care se impun anumite cerinţe şi proiectanţii nu ştiu cum să le satisfacă.

Iată care sînt principalele elemente care trebuie specificate în orice proiect :

- Lăţimea de bandă dorită ;
- Gradul maxim de utilizare a reţelei ;
- Gradul optim de utilizare a reţelei ;
- Randamentul reţelei (throughput-ul) ;
- Acurateţea traficului ;
- Latenţa ;
- Timpul de răspuns

Gradul de utilizare a reţelei este exprimat de cele mai multe ori ca procent din lăţimea de bandă a acesteia. În baza cercetărilor făcute de către IEEE, se consideră că în reţelele Ethernet care folosesc medii partajate, gradul mediu de utilizare nu trebuie să depăşească 37% din lăţimea disponibilă. Peste această valoare se consideră că rata coliziunilor nu mai poate fi acceptată. Pentru reţele FDDI, procentul acceptat este de 70%.

Pentru mulţi utilizatori, indicatorul cel mai la îndemînă este timpul de răspuns. Afirmaţii de genul „reţeaua merge greu" se aud în mod frecvent. Cînd pentru o aplicaţie banală acest timp este mai mare de 100 ms, înseamnă că în reţea sînt probleme. Această valoare se aplică în general aplicaţiilor interactive. Pentru transferul de fişiere cu dimensiuni impresionante sau pagini Web cu grafică în exces, acest timp poate să ajungă pînă la cîteva zeci de secunde.

Cei mai mulţi producători de echipamente specifică pentru produsele lor numărul de pachete pe secundă (PPS) pe care acestea le pot procesa. Aceste valori reprezintă de fapt *throughput*-ul la nivel de echipament : numărul maxim de pachete pe care le poate transmite fără erori. Este un indicator important de care trebuie ţinut cont în selectarea dispozitivelor de reţea.

Există şi un throughput la nivel de aplicaţie. Ca şi în cazul reţelei, şi acesta poate afecta performanţa, dar, din fericire, aici efectele se datorează altor factori : rata de transfer a hard discului, bus-ul calculatorului, timpul de acces al memoriei, procesorul etc.

Acurateţea se referă la biţii care traversează mediile de transmisie de la sursă la destinaţie. Sînt destul de dificil de identificat astfel de probleme, deoarece majoritatea analizoarelor de trafic se ocupă de cadrele care traversează reţeaua şi mai puţin de biţi. Chiar şi aşa, în baza informaţiilor oferite de aceste aplicaţii, puteţi compara numărul de cadre ce conţin erori din totalul numărului de cadre transmise în reţea.

6. *Cerinţele specifice utilizatorilor*

Se referă la orice altă specificaţie raţională care vine din partea utilizatorilor.

Caracteristici ale traficului într-o reţea

În cele ce urmează, vom prezenta cîteva din valorile relative la traficul unei reţele pentru a vă face o idee despre impactul tehnologiilor existente asupra unui astfel de proiect. Ştiţi deja că transferul de informaţii sub formă de text nu va consuma aceleaşi resurse ca o discuţie prin intermediul unei camere Web.

Numărul pachetelor care circulă în reţea la iniţializarea unui client NetBIOS sînt prezentate în tabelul următor :

Tabelul 12.1.3. Caracterizarea traficului reţelei pentru un client NetBIOS

Pachet	Sursă	Destinaţie	Mărimea pachetului în bytes	Numărul de pachete	Numărul total de bytes
Verificare nume	Client	Broadcast	44	6	264
Căutare nume pentru fiecare server	Client	Broadcast	44	Depinde de numărul de servere	44 (dacă este doar un server)
Răspunsul la căutarea numelui	Server	Client	44	Depinde de numărul de servere	44 (dacă este doar un server)
Iniţializare sesiune pentru fiecare server	Client	Server	14	Depinde de numărul de servere	14 (dacă este doar un server)
Confirmarea sesiunii	Server	Client	14	Depinde de numărul de servere	14 (dacă este doar un server)

În cazul unei sesiuni TCP/IP, la iniţializarea unui client situaţia se prezintă după cum urmează :

Tabelul 12.1.4. Caracterizarea traficului reţelei pentru o sesiune TCP/IP

Pachet	Sursă	Destinaţie	Mărimea pachetului în bytes	Numărul de pachete	Numărul total de bytes
Cererea ARP pentru verificarea unicităţii adresei	Client	Broadcast	28	1	28
Cerere ARP către fiecare server	Client	Broadcast	28	Depinde de numărul de servere	Depinde de numărul de servere
Cerere ARP către un router	Client	Broadcast	28	1	28
Răspunsul la cererea ARP	Server/router	Client	28	1	28

Dacă în reţea clienţii folosesc DHCP, la informaţiile prezentate anterior se mai adaugă:

Tabelul 12.1.5. Caracterizarea traficului reţelei pentru un client DHCP

Pachet	Sursă	Destinaţie	Mărimea pachetului în bytes	Numărul de pachete	Numărul total de bytes
Căutarea DHCP	Client	Broadcast	576	O dată la cîteva secunde, pînă cînd serverul este găsit	depinde
Oferta DHCP	Server	Broadcast	328	1	328
Cererea DHCP	Client	Broadcast	576	1	576
DHCP ACK	Server	Broadcast	328	1	328

În această situaţie, cererea prin care un client verifică unicitatea adresei va conţine 3 pachete.

12.2. Securitatea reţelei[1]

Nu ne-am propus să acoperim în cîteva pagini un subiect despre care se scriu cărţi specializate. În primul rînd, este foarte posibil ca pînă la apariţia acestor rînduri să se fi înregistrat lucruri noi în domeniu. Şi asta deoarece „băieţii răi" sînt mai mulţi decît „băieţii buni". Vom face însă o prezentare a celor mai comune atacuri, dar şi a metodelor de protecţie a reţelelor.

Metodele prin care se încearcă pătrunderea neautorizată într-o reţea sînt diverse. La început, majoritatea politicilor de securitate se îndreptau împotriva atacurilor din exteriorul firmei. Astăzi se consideră că neprotejarea sistemului şi împotriva atacurilor din interiorul organizaţiei reprezintă o mare eroare.

12.2.1. Aspecte legislative

Avînd în vedere gradul de sensibilitate a subiectului pe care încercăm să îl tratăm în acest paragraf, considerăm că este necesar să ştiţi că există o lege care sancţionează activităţile ilicite dintr-o reţea: **LEGEA nr. 161 din 19 aprilie 2003 privind unele măsuri pentru asigurarea transparenţei în exercitarea demnităţilor publice, a funcţiilor publice şi în mediul de afaceri, prevenirea şi sancţionarea corupţiei face referire şi la criminalitatea informatică.**

1. Pentru mai multe detalii legate de securitate sistemelor informaţionale, vezi şi D. Oprea, *Protecţia şi securitatea sistemelor informaţionale*, Editura Polirom, Iaşi, 2002.

TITLUL III: Prevenirea şi combaterea criminalităţii informatice

CAPITOLUL I: Dispoziţii generale

Art. 34

Prezentul titlu reglementează prevenirea şi combaterea criminalităţii informatice, prin măsuri specifice de prevenire, descoperire şi sancţionare a infracţiunilor săvîrşite prin intermediul sistemelor informatice, asigurîndu-se respectarea drepturilor omului şi protecţia datelor personale.

Art. 35

(1) În prezentul titlu, termenii şi expresiile de mai jos au următorul înţeles:

a) prin sistem informatic se înţelege orice dispozitiv sau ansamblu de dispozitive interconectate sau aflate în relaţie funcţională, dintre care unul sau mai multe asigură prelucrarea automată a datelor, cu ajutorul unui program informatic;
b) prin prelucrare automată a datelor se înţelege procesul prin care datele dintr-un sistem informatic sînt prelucrate prin intermediul unui program informatic;
c) prin program informatic se înţelege un ansamblu de instrucţiuni care pot fi executate de un sistem informatic în vederea obţinerii unui rezultat determinat;
d) prin date informatice se înţelege orice reprezentare a unor fapte, informaţii sau concepte într-o formă care poate fi prelucrată printr-un sistem informatic. În această categorie se include şi orice program informatic care poate determina realizarea unei funcţii de către un sistem informatic;
e) prin furnizor de servicii se înţelege:
   1. orice persoană fizică sau juridică ce oferă utilizatorilor posibilitatea de a comunica prin intermediul sistemelor informatice;
   2. orice altă persoană fizică sau juridică ce prelucrează sau stochează date informatice pentru persoanele prevăzute la pct. 1 şi pentru utilizatorii serviciilor oferite de acestea;
f) prin date referitoare la traficul informaţional se înţelege orice date informatice referitoare la o comunicare realizată printr-un sistem informatic şi produse de acesta, care reprezintă o parte din lanţul de comunicare, indicînd originea, destinaţia, ruta, ora, data, mărimea, volumul şi durata comunicării, precum şi tipul serviciului utilizat pentru comunicare;
g) prin date referitoare la utilizatori se înţelege orice informaţie care poate conduce la identificarea unui utilizator, incluzînd tipul de comunicaţie şi serviciul folosit, adresa poştală, adresa geografică, numere de telefon sau alte numere de acces şi modalitatea de plată a serviciului respectiv, precum şi orice alte date care pot conduce la identificarea utilizatorului;
h) prin măsuri de securitate se înţelege folosirea unor proceduri, dispozitive sau programe informatice specializate, cu ajutorul cărora accesul la un sistem informatic este restricţionat sau interzis pentru anumite categorii de utilizatori;
i) prin materiale pornografice cu minori se înţelege orice material care prezintă un minor avînd un comportament sexual explicit sau o persoană majoră care este prezentată ca un minor avînd un comportament sexual explicit ori imagini care,

- deşi nu prezintă o persoană reală, simulează, în mod credibil, un minor avînd un comportament sexual explicit.

(2) În sensul prezentului titlu, acţionează fără drept persoana care se află în una dintre următoarele situaţii:

a) nu este autorizată, în temeiul legii sau al unui contract;
b) depăşeşte limitele autorizării;
c) nu are permisiunea, din partea persoanei fizice sau juridice competente, potrivit legii, de a acorda, de a folosi, administra sau controla un sistem informatic ori de a desfăşura cercetări ştiinţifice sau de a efectua orice altă operaţiune într-un sistem informatic.

CAPITOLUL II: Prevenirea criminalităţii informatice

Art. 36

Pentru asigurarea securităţii sistemelor informatice şi a protecţiei datelor personale, autorităţile şi instituţiile publice cu competenţe în domeniu, furnizorii de servicii, organizaţiile neguvernamentale şi alţi reprezentanţi ai societăţii civile desfăşoară activităţi comune şi programe de prevenire a criminalităţii informatice.

Art. 37

Autorităţile şi instituţiile publice cu competenţe în domeniu, în cooperare cu furnizorii de servicii, organizaţiile neguvernamentale şi alţi reprezentanţi ai societăţii civile promovează politici, practici, măsuri, proceduri şi standarde minime de securitate a sistemelor informatice.

Art. 38

Autorităţile şi instituţiile publice cu competenţe în domeniu, în cooperare cu furnizorii de servicii, organizaţiile neguvernamentale şi alţi reprezentanţi ai societăţii civile organizează campanii de informare privind criminalitatea informatică şi riscurile la care sînt expuşi utilizatorii de sisteme informatice.

Art. 39

(1) Ministerul Justiţiei, Ministerul de Interne, Ministerul Comunicaţiilor şi Tehnologiei Informaţiei, Serviciul Român de Informaţii şi Serviciul de Informaţii Externe constituie şi actualizează continuu baze de date privind criminalitatea informatică.

(2) Institutul Naţional de Criminologie din subordinea Ministerului Justiţiei efectuează studii periodice în scopul identificării cauzelor care determină şi a condiţiilor ce favorizează criminalitatea informatică.

Art. 40

Ministerul Justiţiei, Ministerul de Interne, Ministerul Comunicaţiilor şi Tehnologiei Informaţiei, Serviciul Român de Informaţii şi Serviciul de Informaţii Externe desfăşoară programe speciale de pregătire şi perfecţionare a personalului cu atribuţii în prevenirea şi combaterea criminalităţii informatice.

Art. 41

Proprietarii sau administratorii de sisteme informatice, la care accesul este interzis sau restricţionat pentru anumite categorii de utilizatori, au obligaţia de a avertiza utilizatorii cu privire la condiţiile legale de acces şi utilizare, precum şi cu privire la

consecințele juridice ale accesului fără drept la aceste sisteme informatice. Avertizarea trebuie să fie accesibilă oricărui utilizator.

CAPITOLUL III: Infracțiuni și contravenții

SECȚIUNEA 1: Infracțiuni contra confidențialității și integrității datelor și sistemelor informatice

Art. 42

(1) Accesul, fără drept, la un sistem informatic constituie infracțiune și se pedepsește cu închisoare de la 3 luni la 3 ani sau cu amendă.

(2) Fapta prevăzută la alin. (1), săvîrșită în scopul obținerii de date informatice, se pedepsește cu închisoare de la 6 luni la 5 ani.

(3) Dacă fapta prevăzută la alin. (1) sau (2) este săvîrșită prin încălcarea măsurilor de securitate, pedeapsa este închisoarea de la 3 la 12 ani.

Art. 43

(1) Interceptarea, fără drept, a unei transmisii de date informatice care nu este publică și care este destinată unui sistem informatic, provine dintr-un asemenea sistem sau se efectuează în cadrul unui sistem informatic constituie infracțiune și se pedepsește cu închisoare de la 2 la 7 ani.

(2) Cu aceeași pedeapsă se sancționează și interceptarea, fără drept, a unei emisii electromagnetice provenite dintr-un sistem informatic ce conține date informatice care nu sînt publice.

Art. 44

(1) Fapta de a modifica, șterge sau deteriora date informatice ori de a restricționa accesul la aceste date, fără drept, constituie infracțiune și de pedepsește cu închisoare de la 2 la 7 ani.

(2) Transferul neautorizat de date dintr-un sistem informatic se pedepsește cu închisoare de la 3 la 12 ani.

(3) Cu pedeapsa prevăzută la alin. (2) se sancționează și transferul neautorizat de date dintr-un mijloc de stocare a datelor informatice.

Art. 45

Fapta de a perturba grav, fără drept, funcționarea unui sistem informatic, prin introducerea, transmiterea, modificarea, ștergerea sau deteriorarea datelor informatice sau prin restricționarea accesului la aceste date constituie infracțiune și se pedepsește cu închisoare de la 3 la 15 ani.

Art. 46

(1) Constituie infracțiune și se pedepsește cu închisoare de la 1 la 6 ani:

a) fapta de a produce, de a vinde, de a importa, de a distribui sau de a pune la dispoziție, sub orice altă formă, fără drept, un dispozitiv sau program informatic conceput sau adaptat în scopul săvîrșirii uneia dintre infracțiunile prevăzute la art. 42-45;

b) fapta de a produce, de a vinde, de a importa, de a distribui sau de a pune la dispoziție, sub orice altă formă, fără drept, o parolă, cod de acces sau alte asemenea date informatice care permit accesul total sau parțial la un sistem informatic în scopul săvîrșirii uneia dintre infracțiunile prevăzute la art. 42-45.

(2) Cu aceeaşi pedeapsă se sancţionează şi deţinerea, fără drept, a unui dispozitiv, program informatic, parolă, cod de acces sau dată informatică dintre cele prevăzute la alin. (1) în scopul săvîrşirii uneia dintre infracţiunile prevăzute la art. 42-45.

Art. 47

Tentativa infracţiunilor prevăzute la art. 42-46 se pedepseşte.

SECŢIUNEA 2: Infracţiuni informatice

Art. 48

Fapta de a introduce, modifica sau şterge, fără drept, date informatice ori de a restricţiona, fără drept, accesul la aceste date, rezultînd date necorespunzătoare adevărului, în scopul de a fi utilizate în vederea producerii unei consecinţe juridice, constituie infracţiune şi se pedepseşte cu închisoare de la 2 la 7 ani.

Art. 49

Fapta de a cauza un prejudiciu patrimonial unei persoane prin introducerea, modificarea sau ştergerea de date informatice, prin restricţionarea accesului la aceste date ori prin împiedicarea în orice mod a funcţionării unui sistem informatic, în scopul de a obţine un beneficiu material pentru sine sau pentru altul, constituie infracţiune şi se pedepseşte cu închisoare de la 3 la 12 ani.

Art. 50

Tentativa infracţiunilor prevăzute la art. 48 şi 49 se pedepseşte.

SECŢIUNEA 3: Pornografia infantilă prin sisteme informatice

Art. 51

(1) Constituie infracţiune şi se pedepseşte cu închisoare de la 3 la 12 ani şi interzicerea unor drepturi, producerea în vederea răspîndirii, oferirea sau punerea la dispoziţie, răspîndirea sau transmiterea, procurarea pentru sine sau pentru altul de materiale pornografice cu minori prin sisteme informatice ori deţinerea, fără drept, de materiale pornografice cu minori într-un sistem informatic sau un mijloc de stocare a datelor informatice.

(2) Tentativa se pedepseşte.

SECŢIUNEA 4: Contravenţii

Art. 52

Nerespectarea obligaţiei prevăzute la art. 41 constituie contravenţie şi se sancţionează cu amendă de la 5.000.000 lei la 50.000.000 lei.

Art. 53

(1) Constatarea contravenţiei prevăzute la art. 52 şi aplicarea sancţiunii se fac de către personalul împuternicit în acest scop de către ministrul comunicaţiilor şi tehnologiei informaţiei, precum şi de către personalul special abilitat din cadrul Ministerului de Interne.

(2) Contravenţiei prevăzute la art. 52 îi sînt aplicabile dispoziţiile Ordonanţei Guvernului nr. 2/2001 privind regimul juridic al contravenţiilor, aprobată cu modificări şi completări prin Legea nr. 180/2002, cu modificările ulterioare.

Înainte de a prezenta principalele categorii de atacuri și modalitățile de realizare a acestora, facem o precizare. Dacă nu ați mai folosit astfel de aplicații înainte, încercați să nu le testați într-o rețea cu ieșire la Internet. Dacă din greșeală scanați un calculator care nu vă privește, este posibil să fiți luat drept hacker, iar activitatea dumneavoastră să fie considerată infracțiune. Prin urmare, scanați doar calculatoarele din rețeaua dumneavoastră și informați utilizatorii și/sau șefii cu privire la acțiunile dumneavoastră !

Riscăm cu această prezentare, pentru că multe dintre aceste aplicații, dacă sînt folosite în mod pașnic, reprezintă un instrumnet foarte bun pentru îmbunătățirea securității propriei rețele !

12.2.2. Tipuri de atacuri într-o rețea[1]

1. *Scanning (scanarea)*

Scanarea unei rețele poate fi privită din două puncte de vedere.

În primul rînd, scanarea poate fi procesul prin care sînt transmise informații către dispozitivele din rețea pentru a primi un răspuns cît mai explicit din partea acestora, răspuns în baza căruia să poată fi identificată structura rețelei. În al doilea rînd, scanarea poate presupune identificarea vulnerabilităților existente într-o rețea cu scopul de a le elimina/reduce.

În majoritatea cazurilor, atacatorul nu cunoaște structura și/sau topologia rețelei pe care dorește să o compromită sau să o atace.

Prima etapă constă în culegerea de informații cu scopul de a schița harta rețelei (*network mapping*). Pentru aceasta este nevoie să se identifice calculatoarele active și serviciile pe care acestea le rulează. Atacatorul face apel la aplicații specilizate în acest sens.

În următoarea etapă, el va încerca să obțină cît mai multe informații despre stațiile identificate ca fiind active în rețea: numele conturilor folosite, resursele partajate în rețea, aplicațiile deschise etc. Chiar dacă multe informații obținute par inofensive la prima vedere, ele pot fi folosite pentru a afla vulnerabilitățile sistemului de operare sau aplicațiile rulate.

Accesul neautorizat într-o rețea se obține, de obicei, pe două căi : prin intermediul unui nume de utilizator și o parolă valide sau prin folosirea abuzivă a privilegiilor utilizatorilor. Analiza parolelor sau, mai bine zis, folosirea unor programe pentru spargerea parolelor poate da rezultate satisfăcătoare.

- **SuperScan** este o aplicație cu interfață grafică ce oferă o paletă destul de bogată de opțiuni de scanare. În plus, nici nu trebuie să ai prea multe cunoștințe. Este de ajuns să știi o adresă IP (sau mai multe) și ce reprezintă porturile scanate.

---

1. Subiectul este tratat în detaliu în *Hack Proofing yor Network*, Syngress 2002, cu exemple mai multe pentru Unix/Linux.

- **Winfingerprint** este o aplicaţie care rulează pe platformă Windows, capabilă să determine sistemul de operare, utilizatorii sau grupurile de utilizatori, serviciile şi logurile. Partea mai intereseantă este că această aplicaţie are posibilitatea de a specula sesiunile nule care pot fi create pe maşinile Windows, dacă această posibilitate nu a fost anulată de către administrator.

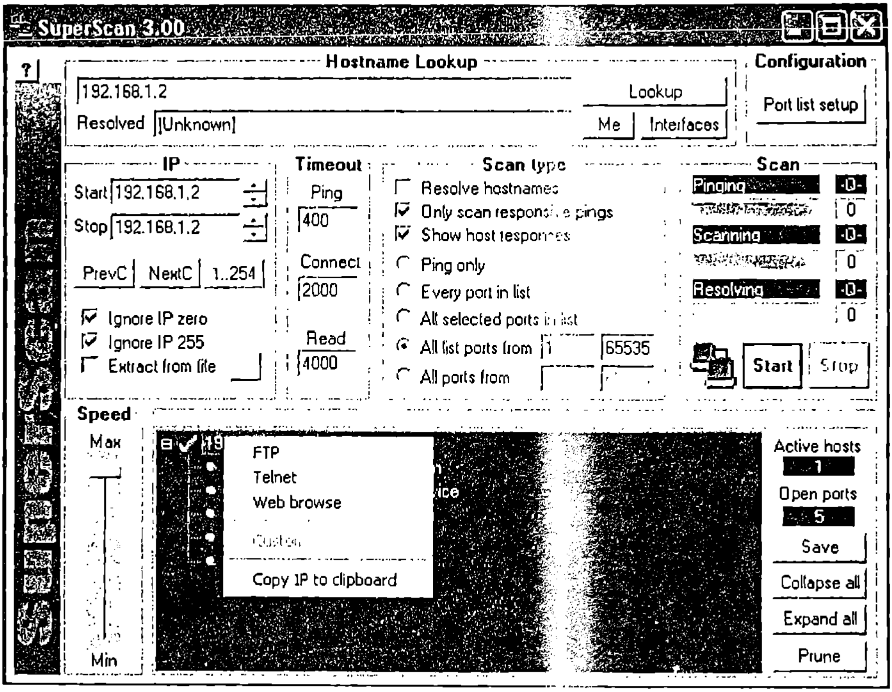


Figura 12.2.1. SuperScan

- **LC4** este ultima variantă a celei mai populare aplicaţii pentru spart parolele maşinilor Windows : LOphtcrack. Noua variantă oferă date statistice cu privire la timpul necesar spargerii parolei fiecărui cont în parte, modalităţi de obţinere a parolelor criptate (în Windows 2000 şi XP acestea sînt păstrate sub formă criptată).

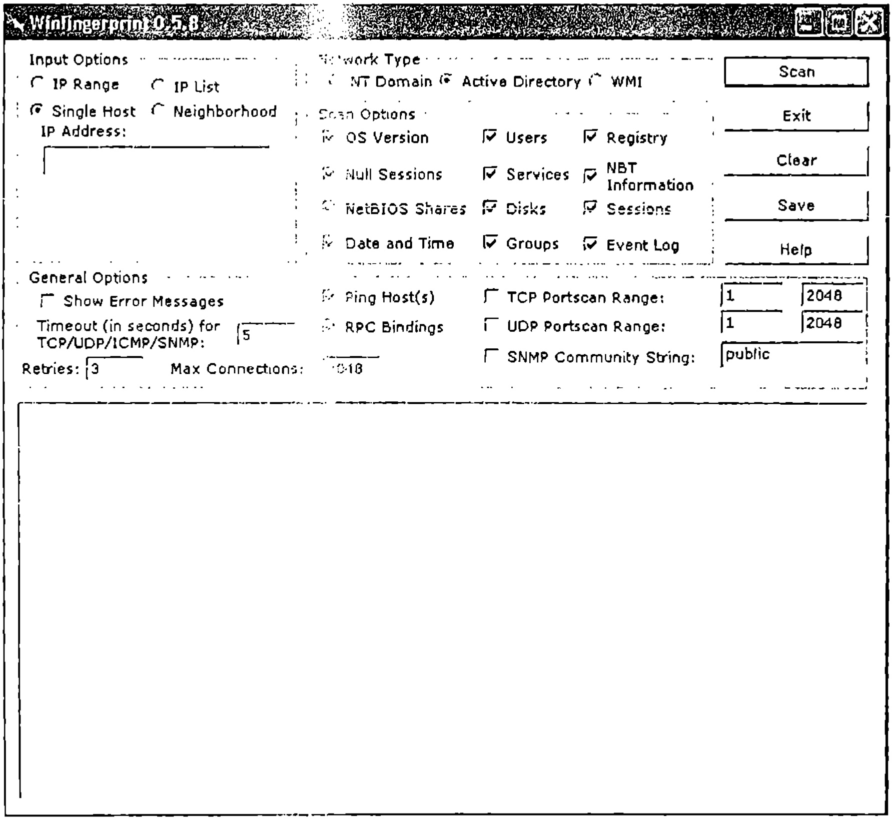


Figura 12.2.2. Winfingerprint

- **NMAP (Network Mapper)** este un utilitar pentru explorarea reţelei şi auditarea securităţii acesteia. Aplicaţia identifică ce staţii sînt active într-o reţea, care sînt serviciile (porturile) deschise pe acele staţii, ce sistem de operare rulează (inclusiv versiunea), dacă este folosit un firewall sau altă aplicaţie pentru filtrarea pachetelor etc. Este disponibilă atît în versiune grafică, cît şi în varianta consolă. Lucrează silenţios, fiind destul de greu de descoperit (*stealth scanner*).

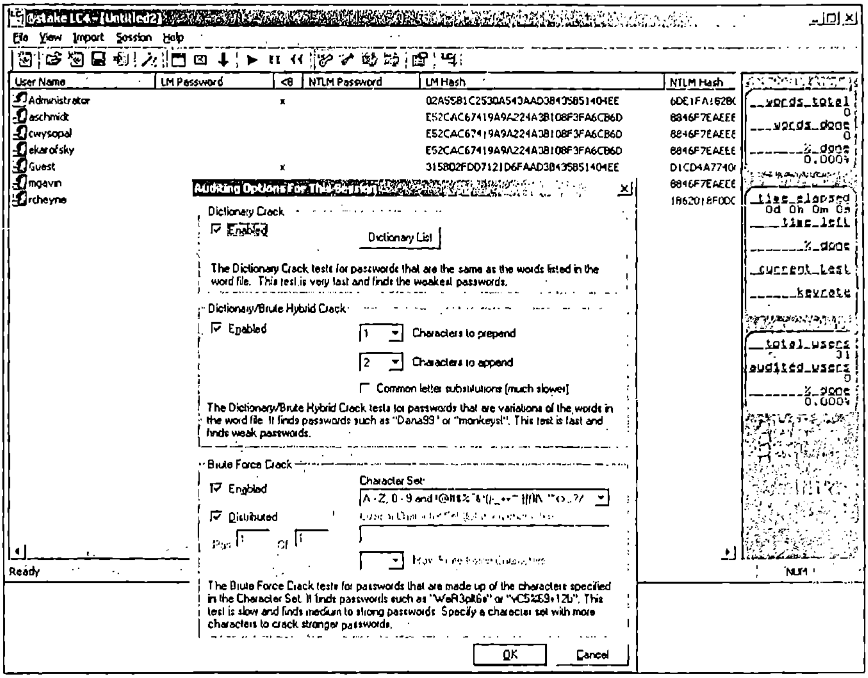


Figura 12.2.3. LC4

Lista ar putea continua, dar ne oprim aici. Pentru a vă testa vulnerabilităţile din reţea puteţi apela şi la o firmă specializată pentru a vă scana reţeaua din exterior. Dacă însă nu veţi lua în calcul şi eventualele probleme care pot să apară chiar de la propriii angajaţi, s-ar putea ca mai tîrziu să aveţi surprize nu chiar plăcute.

2. *Denial of Service (DoS)*

Reprezintă încercarea explicită a unui intrus de a împiedica utilizatorii să folosească un serviciu asupra căruia au drepturi. În documentele CERT (Computer Emergency Response Team) se spune că atacurile de tip DoS au trei forme generale de manifestare :

- utilizarea neautorizată a unor resurse limitate ;
- distrugerea sau alterarea informaţiilor ;
- distrugerea sau alterarea componentelor unei reţele.

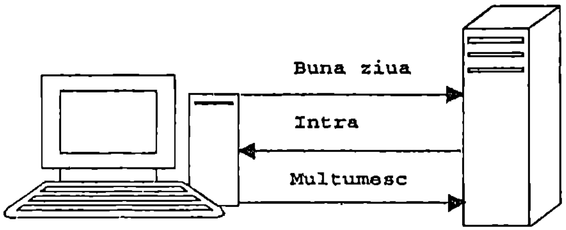
Dacă grupăm cele spuse de CERT, ajungem să vorbim despre două tipuri de atacuri DoS : *atacarea sistemelor de operare* şi *atacarea reţelei*. În primul caz, se au în vedere vulnerabilităţile sistemului de operare. Aceasta este şi cea mai cunoscută variantă a acestui tip de atac. De obicei, problemele acestea sînt rezolvate prin patch-urile sau service-pack-urile pe care le pune la dispoziţia utilizatorilor producătorul respectivului SO.

În cel de al doilea caz însă, atacul se bazează pe limitările inerente care există într-o rețea, limitări care țin mai ales de tehnologie. Atacurile împotriva unor site-uri precum Amazon sau Yahoo au demonstrat că pînă şi cei mai mari au probleme. Oricîte clasificări se fac însă, toată lumea e de acord că *buffer overflow, syn, teardrop* sau *smurf* sînt atacuri de tip DoS.

Buffer Overflow

Ce poate fi mai simplu decît să generezi către o adresă de rețea un trafic mai mare decît poate duce buffer-ul programului receptor? Cel care încearcă acest lucru nu trebuie să cunoască neapărat exploit-ul sistemului țintă. Atacă pur şi simplu, poate merge. Cel mai cunoscut atac care se baza pe caracteristicile buffer-ului unui program/sistem este *ping of death* – transmiterea de pachete ICMP mai mari decît 65,527 octeți (se foloseşte un utilitar care *ştie* să creeze astfel de pachete).

SYN Attack (SYN flooding)



Vă mai amintiți ce presupunea stabilirea unei conexiuni TCP? Stația sursă transmite către server un mesaj prin care cere să se autentifice (mesaj SYN). Serverul returnează aprobarea (mesaj SYN-ACK), iar stația sursă confirmă recepționarea acesteia (mesaj ACK). Atacul poate să apară în momentul în care serverul răspunde clientului cu mesajul SYN-ACK, dar nu primeşte de la acesta mesajul ACK, speculîndu-se timpul necesar *schimbului de amabilități* dintre cele două sisteme. Pachetele care se transmit în timpul stabilirii conexiunii includ un cîmp SYN care identifică numărul secvenței din cadrul mesajului. Cererile de conexiune TCP (SYN-ul) sînt transmise calculatorului țintă. Adresa sursă din pachetul cerere este înlocuită cu o altă adresă (de exemplu, a altui calculator). Calculatorul care recepționează cererea răspunde cu un mesaj SYN-ACK către adresa identificată în cerere, dar nu primeşte nici un ACK din partea acestei stații pentru că nu este ea cea care a lansat cererea. O maşină Windows retransmite mesajul SYN-ACK de cinci ori dublînd valoarea time-out la fiecare încercare. Inițial, valoarea time-out este de 3 secunde, deci încercările vor dura 3, 6, 12, 24 şi 48 secunde!

Dacă există suspiciuni că sistemul este supus unui atac SYN, se pot verifica conexiunile cu ajutorul comenzii **netstat -n -p tcp**. Dacă sînt afişate prea multe conexiuni a căror stare este SYN-RECEIVED, există posibilitatea ca sistemul să fie atacat.

Această problemă ține mai mult de setările sistemului de operare: mărimea buffer-ului şi perioada de time-out. Atacatorul lucrează de pe mai multe maşini: una de pe care coordonează atacul şi mai multe de pe care lansează cererile.

Teardrop

Atacul se bazează pe modul în care are loc reasamblarea packetelor IP la destinaţie. Fragmentarea apare ca răspuns la diferitele tipuri de reţele pe care le traversează un mesaj pentru a ajunge la destinaţie. Atît mediile de transmisie, cît şi protocoalele au reguli diferite în ceea ce priveşte mărimea maximă a datagramelor care le traversează (MTU). Prin urmare, o datagramă care are o MTU mai mare decît a pachetului ce trebuie transmis va fi fragmentată. Pentru a putea fi reasamblat la destinaţie, un pachet care a fost fragmentat conţine în headerul IP următoarele informaţii: id-ul fragmentului, poziţia în cadrul pachetului original (cîmpul se numeşte offset, are o lungime de 13 biţi, şi pentru primul fragment are valoarea 0), lungimea datelor transportate şi dacă după el mai există alte fragmente.

Un astfel de atac implică modificarea valorii cîmpului offset din cel de al doilea fragment (sau din următoarele) astfel încît sistemul staţiei destinatare să nu poată reasambla fragmentele.

Smurf

Această variantă de atac DoS presupune trimiterea unei cereri ping de pe maşina ţintă către adresa de broadcast a reţelei din care face parte. Staţiile din reţeaua victimei vor genera pachetul de răspuns către staţia acesteia, inundînd reţeaua cu pachete ICMP (transmiterea unui pachet cu altă adresă sursă decît cea de origine se numeşte *spoofing*).

O formă mult mai complexă o reprezintă atacurile DoS distribuite (DDoS), care se bazează pe modelul client server. Intrusul atacă şi preia controlul unui număr mic de staţii de pe care controlează un număr mai mare de staţii din domeniul lor. Aceste din urmă staţii lansează simultan sau grupat, în mod controlat şi susţinut, atacuri către calculatorul *victimă*.

3. *Sniffing*

Sniffing (ascultarea porturilor de comunicaţie) sau **man-in-the-middle** este atacul prin care atacatorul afectează securitatea reţelei într-o manieră pasivă.

Spuneam despre cartela de reţea că recepţionează şi interpretează doar pachetele care îi sînt destinate (conţin adresa MAC respectivă), celelalte fiind ignorate. Cartelele pot funcţiona însă şi în modul *promiscuous*, care le permite să recepţioneze tot traficul din reţea.

Ce informaţii interesează? Multe dintre informaţiile conţinute în pachetele TCP/IP sînt reziduale pentru un hacker, dar uneori pot conţine informaţii despre numele de utilizator, parole, conţinuturi ale e-mail-urilor. Mai ales dacă transmisia nu este criptată!

Prin urmare, cel mai adesea se urmăresc porturile pe care rulează aplicaţii în care autentificarea utilizatorilor nu este securizată: telnet (portul 23), ftp (portul 21), IMAP (Internet Message Access Protocol lucrează pe portul 143), http (portul 80).

Dintre aplicaţiile dedicate acestor activităţi amintim:

- **NetworkActiv Sniffer** permite captarea şi analizarea pachetelelor IP, filtrarea acestora după adresă IP-port-protocol. Opţiunea *File Sniffer* permite captura de fişiere HTTP (pagini Web, poze, download-uri).

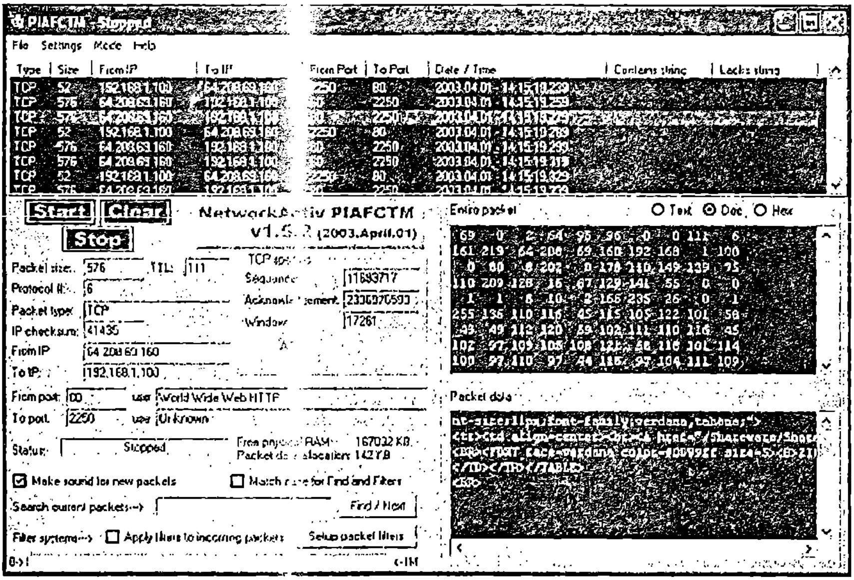


Figura 12.2.4. NetworkActiv PIAFCTM

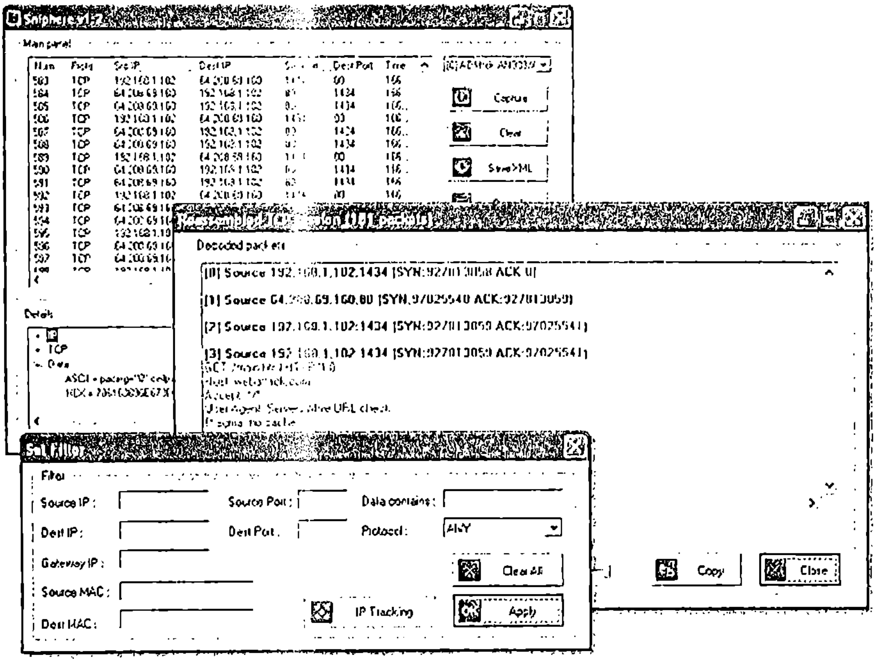


Figura 12.2.5. Sniphere

- **Sniphere** este un alt sniffer de reţea care permite filtrarea pachetelor captate în funcţie de adresa IP, adresa MAC, porturile sau protocoalele dorite. Decodează pachetele captate.
- **Ethereal Network Analyzer** oferă posibilitatea de a vizualiza în detaliu fiecare pachet. Facilitatea care îl deosebeşte de celelalte este posibilitatea de a vizualiza şi reface o sesiune TCP, putînd citi pachetele captate cu alte utilitare de acest gen.

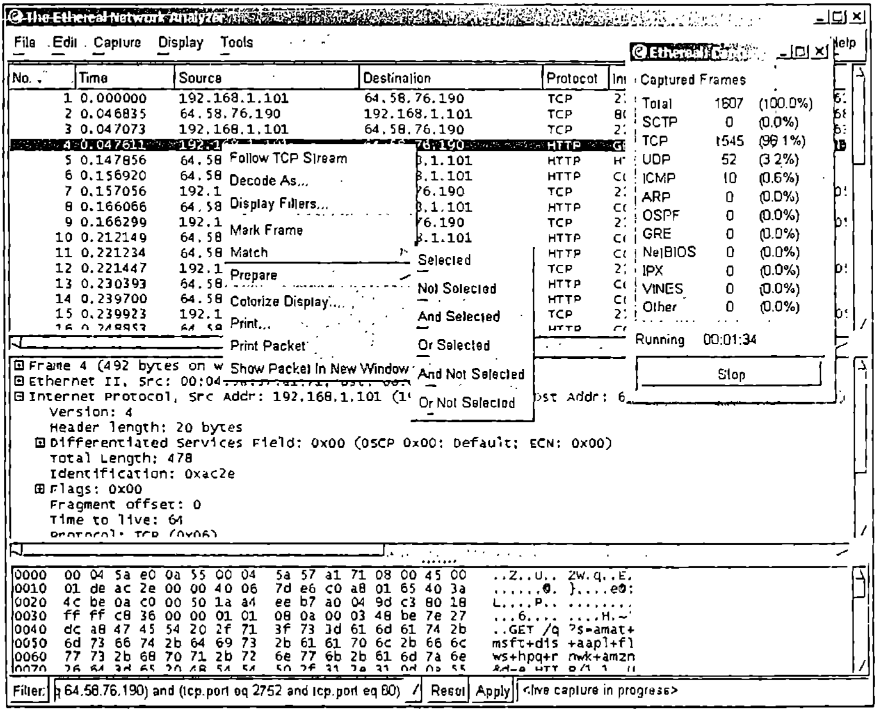


Figura 12.2.6. Ethereal Network Analyzer

Cînd se va încerca monitorizarea unei reţele în care există switch-uri, majoritatea aplicaţiilor de mai sus nu vor putea depăşi segmentul de reţea din care face parte calculatorul de pe care rulează. În acest caz, trebuie folosite aplicaţii care au posibilitatea de a asculta tabelele ARP ale switch-urilor sau care captează traficul direct din router.

4. *Hijacking*

Hijacking (piraterie sau deturnare) reprezintă o altă variantă de man-in-the-middle ce presupune substituirea unei identităţi pentru a avea acces la informaţii. Este un atac activ, care necesită însă un efort mai mare din partea atacatorului şi o înţelegere exactă a modului în care funcţionează o sesiune TCP sau UDP. Pătrunderea în reţea se face prin intermediul unui utilizator autorizat. Atacul efectiv poate începe prin bombardarea cu

pachete (DoS) a unei staţii autorizate, eliminarea sa din reţea şi configurarea propriei staţii cu setările staţiei atacate.

Majoritatea aplicaţiilor de tip IDS (*Intrusion Detection System*) detectează aceste tipuri de atacuri.

5. *Atacul pe uşile din spate (backdoors)*

Presupune apelarea la o subrutină nedocumentată din anumite aplicaţii sau prin intermediul unei parole „uitate" de realizatorul aplicaţiei respective. Cele mai multe atacuri rămîn necunoscute, dar dacă sînt descoperite, constituie o gravă problemă de securitate.

Dintre utilitare care identifică „găurile" dintr-un sistem amintim:

- **Verified Security PC Center** - este un ansamblu de 6 aplicaţii dintre care cele mai importante sînt detectarea cailor troieni, mecanisme de apărare împotriva hackerilor şi monitorizarea traficului. Poate cripta fişiere sau directoare şi oferă posibilitatea analizării securităţii sistemului pentru a detecta posibilele puncte slabe.

Figura 12.2.7. Verified Security PC

- **Tauscan** este un scanner de cai troieni capabil să detecteze şi să elimine majoritatea viruşilor de acest tip. Rulează în background şi se actualizează singur cu ultimele definiţii.

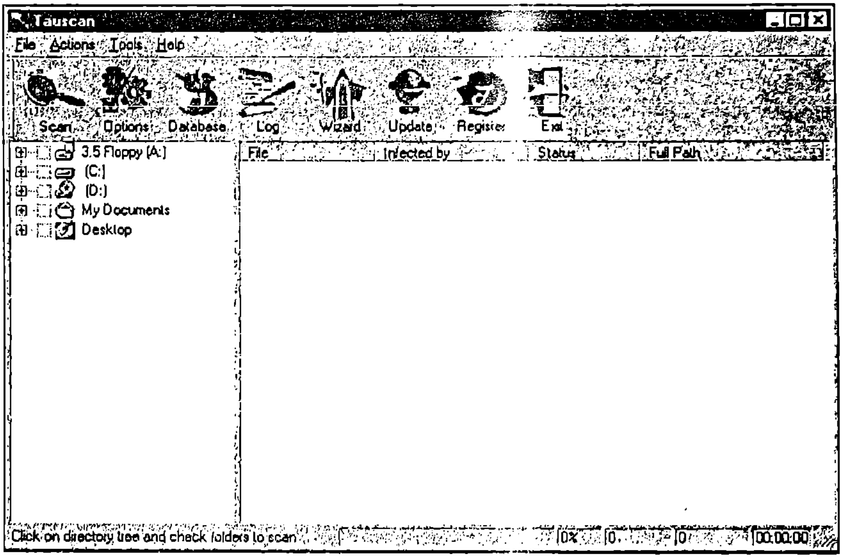


Figura 12.2.8. Tauscan

12.2.3. Mecanisme de protecţie

1. *Firewall*[1]

Pentru un administrator de reţea este foarte important să cunoască cele mai bune mecanisme prin care poate realiza o politică de securitate cît mai bine adaptată specificului firmei sale.

Firewall-ul poate fi considerat un sistem sau un ansamblu de sisteme care asigură securitatea reţelei interne în relaţie cu celelalte reţele cu care intră în contact. Din punct de vedere fizic, el poate fi un simplu PC sau staţie de lucru, un router sau chiar un mainframe. Din punct de vedere logic, el determină care sînt informaţiile sau serviciile care pot fi accesate din afara reţelei locale şi cine are dreptul de a utiliza aceste resurse.

Ca localizare, firewall este amplasat, în general, în zona în care reţeaua internă face joncţiunea cu cea externă, zonă denumită punct de control. Dacă privim reţeaua ca pe o clădire, firewall este singurul punct prin care se poate intra.

În funcţie de cerinţe, un firewall poate conţine următoarele componente funcţionale care pot fi implementate ca un tot :

- Router pentru filtrarea pachetelor ;
- Gateway la nivel de aplicaţie (proxy) ;
- Gateway la nivel de circuit.

1. O lucrare ce tratează acest subiect găsiţi la http ://secinf.net/firewalls_and_VPN/Firewalls_Complete/.

Routerul pentru filtrarea pachetelor este cel care transmite pachetele în rețea pe baza regulilor de filtrare implementate. Am dat un mic exemplu cînd am prezentat ACL-urile ce pot fi implementate pe un router.

Cînd primește un pachet, routerul poate extrage din antetul său următoarele informații :

- Adresa IP sursă ;
- Adresa IP destinație ;
- Portul TCP/UDP sursă ;
- Portul TCP/UDP destinație ;
- Tipul mesajului ICMP ;
- Informații despre protocolul încapsulat.

În funcție de politica de securitate a firmei se stabilesc și regulile de filtrare. Cel care încearcă să atace rețeaua trebuie să cunoască această politică precum și restricțiile impuse la nivel de serviciu. Cunoscînd numărul porturilor TCP/UDP utilizate de serviciile care rulează în rețea, routerul poate filtra accesul la aceste servicii.

Atunci cînd se cunosc adresele sursă sau destinație, regulile de filtrare de pe router pot accepta sau refuza un pachet în funcție de aceste informații. În cele mai multe cazuri, doar anumite servere pot fi accesate din afara organizației. Pachetelor, care au altă destinație decît adresa IP a respectivelor servere, nu li se va permite accesul în rețeaua locală.

Mecanismele de filtrare mai avansate pot lua în calcul alte opțiuni ale cadrului IP, cum ar fi deplasamentul fragmentului sau cifra de control. Implementarea singulară a acestui mecanism nu oferă însă un grad mare de securitate, cînd rețeaua se dezvoltă și regulile de filtrare devin complexe și greu de gestionat.

Controlul la nivel de aplicație se realizează cel mai adesea prin intermediul unei porți (gateway) sau proxy server. Pe gateway trebuie instalat proxy codul corespunzător fiecărei aplicații care dorește să treacă de poartă.

În timpul unui dialog între un client și un server, proxy-ul acționează ca și server pentru clientul respectiv și devine, la rîndul său, client pentru serverul destinație. Pentru clientul inițial proxy serverul funcționează în mod transparent, dar este capabil să monitorizeze și să filtreze anumite informații sau comenzi. Proxy serverul este un server dedicat aplicațiilor care rulează pe calculatorul ce face legătura dintre rețeaua noastră și restul lumii. Spre deosebire de firewall, el controlează schimbul de informații la nivel de aplicație, și nu de pachet IP.

Dacă luăm ca exemplu protejarea unui server FTP care este accesat din afara rețelei locale, proxy serverul de FTP va fi configurat să nu permită executarea comenzilor PUT sau MPUT.

Pentru ca un client să poată accesa un proxy server, softul client trebuie modificat astfel încît să suporte conexiuni de tip proxy și să se autentifice pe proxy server. Această cerință poate fi considerată ca fiind un dezavantaj al acestui mecanism de protecție.

Pe larg despre acest subiect puteți citi la adresele :

- http : //www2.rad.com/networks/1998/proxy/proxy.htm,
- http : //www.serverwatch.com/tutorials/article.php/10825_1354991_3.

Porțile la nivel de circuit (cunoscute și ca transparent gateway) sînt considerate un caz particular al porților la nivel de aplicație. Aceasta deoarece pot fi configurate să execute anumite operații după ce s-a realizat autentificarea utilizatorului. Chiar dacă gestionează

conexiuni TCP sau UDP, aceste porţi nu filtrează pachetele respective. Ne oprim aici cu prezentarea pentru că un tip de astfel de poartă (SOCKS) îl vom prezenta imediat.

2. *Network Address Translation (NAT)*[1]

NAT sau *masquerading*, cum este denumită această tehnică în mediul Linux, translatează o adresă IP internă (nerutabilă) într-una publică (rutabilă). Mecanismul NAT are la origine două realităţi : pe de o parte, doar o parte dintre calculatoarele unei firme au nevoie de acces în exteriorul reţelei acesteia, iar pe de altă parte, adresele IP publice sînt limitate (şi, în plus, costă).

De cele mai multe ori, calculatoarele folosesc în reţeaua internă adrese IP private, iar pentru dialogul cu calculatoarele din exterior fac apel la NAT/masquerade. Cum funcţionează acest mecanism ?

Pentru fiecare pachet care „iese" din reţeaua locală, maşina pe care este configurat NAT-ul verifică adresa sursă. Dacă aceasta se regăseşte printre regulile implementate, va fi transformată într-o adresă publică dintre cele predefinite. Pentru fiecare pachet care „intră" în reţea NAT verifică dacă are o adresă destinaţie pe care o ştie. Dacă răspunsul este afirmativ, adresa va fi transformată în una internă.

Mecanismul este ceva mai complicat decît ceea ce se vede. Pentru fiecare pachet căruia i se schimbă adresa NAT trebuie să-i modifice şi cifra de control. Dacă ne referim la pachetele FTP, lucrurile se complică şi mai mult, deoarece acestea pot să conţină în cîmpul *date* adrese (comanda *ftp port* conţine o adresă IP în format ASCII, de exemplu).

NAT poate fi implementat pe un firewall, router sau PC şi poate lucra în mai multe moduri :

- **Static NAT** - mapează o adresă IP privată la una publică conform principiului unu-la-unu. Se foloseşte mai ales atunci cînd calculatoarele din reţeaua locală trebuie să fie accesate din exteriorul organizaţiei.
- **Dynamic NAT** - mapează o adresă IP privată la una publică selectată dintr-un grup de adrese.
- **Overloading** - este o formă a NAT-ului dinamic prin care mai multe adrese IP private sînt mapate la o singură adresă IP publică, dar folosind porturi diferite. Această variantă se mai numeşte şi PAT (Port Address Translation) sau NAT multiplexat la nivel de port.

Mai multe detalii puteţi afla citind articolul de la adresa http://computer.howstuffworks.com/nat.htm.

3. *IPSec (Internet Security Protocol)*[2]

IPSec reprezintă setul de protocoale dezvoltate de IETF cu scopul de a securiza schimbul de pachete la nivelul IP. IPSec suportă două modalităţi de criptare : **transport** şi **tunnel**. În modul transport este criptată doar porţiunea cu date a fiecărui pachet, headerul fiind lăsat intact. Modul tunnel este mult mai sigur, deoarece criptează şi headerul pachetului. Pentru a putea fi implementat IPSec, sursa şi destinatarul mesajelor trebuie să partajeze o cheie publică de criptare. Modelul de securitate folosit de IPSec este de tip *end-to-end*

1. Definit prin RFC 1631.
2. Definit prin RFC 2401.

sau, altfel spus, singurele calculatoare care știu despre IPSec sînt sursa și destinatarul datelor transmise prin rețea.

Implementarea IPSec se bazează pe standardele dezvoltate de Internet Engineering Task Force (IETF) și are două obiective principale:

- protejarea pachetelor IP;
- apărarea rețelei împotriva atacurilor.

Ambele obiective sînt atinse prin folosirea serviciilor de protecție bazate pe criptografie, a protocoalelor de securitate și managementul dinamic al cheilor de criptare.

Nu intrăm în amănunte legate de mecanismele interne ale acestui protocol, ci ne vom referi, în continuare, la maniera de implementare în sistemul de operare de la Microsoft. În acest caz, IPSec se bazează pe trei componente: *IPSec policy agent*, *ISAKMP*[1] / *Oakley Key Management Service* și *IPSec driverul*.

IPSec Policy Agent este un mecanism de securitate rezident pe orice mașină W2K. Mai exact, este un serviciu ce pornește automat în momentul startării calculatorului. În funcție de intervalul specificat prin politica IPSec, acest mecanism funcționează astfel:

- încarcă din Active Directory politica IPSec corespunzătoare calculatorului respectiv;
- dacă în Active Directory nu există nici o astfel de politică sau dacă agentul nu se poate conecta la serviciul director (se mai întîmplă), caută politica în regiștrii calculatorului. Dacă nici aici nu găsește o politică, agentul se oprește automat;
- dacă serviciul director identifică o politică de securitate, aceasta este transferată în format criptat calculatorului respectiv. Informațiile din această politică sînt transmise apoi driverului IPSec, serviciului ISAKMP/Oakely și regiștrilor.

ISAKMP/Oakley Key Management Service este tot un mecanism rezident pe fiecare mașină W2K. Înainte ca datagramele IP să fie transmise de la sursă către destinație, între cele două calculatoare trebuie să se realizeze o asociere. Această asociere reprezintă un set de parametri prin care se definesc serviciile de securitate și mecanismele comune ce vor fi folosite pentru protejarea comunicațiilor, cheia de criptare, proprietăți etc.

Protocolul Oakley generează cheile ce vor fi folosite pentru criptarea/decriptarea datelor care se transferă prin rețea. ISAKMP funcționează în două etape:

- mai întîi, stabilește un canal de comunicare sigură între sursă și destinație. Aceasta presupune autentificarea celor două mașini și schimbul datelor care vor alcătui cheia de criptare pe care cele două mașini o vor folosi;
- apoi, realizează asocierea între cele două calculatoare, asociere care este transmisă driverului IPSec de pe cele două mașini, împreună cu cheia de criptare.

Agentul IPSec pornește în mod automat serviciul ISAKMP/Oakley. Dacă între cele două calculatoare nu se poate realiza o asociere, se poate configura o politică IPSec care fie blochează comunicațiile, fie acceptă comunicații despre care nu se știe cît de sigure sînt.

IPSec driver este de fapt fișierul IPSEC.SYS, fișier care există pe orice mașină W2K (C:\WINNT\system32\drivers). Acest driver analizează toate datagramele IP pentru a vedea dacă respectă filtrele impuse prin politica de securitate a calculatorului respectiv. Aceste filtre sînt grupate într-o listă și definesc, în fapt, care sînt calculatoarele și rețelele

1. ISAKMP – Internet Security Association and Key Management Protocol.

care necesită comunicaţii securizate. Cînd condiţiile impuse prin filtre sînt îndeplinite, driverul IPSec de pe calculatorul sursă face apel la asocierea IPSec şi la cheia de criptare. Datele sînt apoi transmise criptat către destinaţie. Aici, driverul IPSsec decriptează datele şi le transmite aplicaţiei care a stat la baza transmisiei.

4. *SOCKS*[1]

După cum spuneam cîteva pagini mai înainte, acesta este un protocol folosit pentru gateway-urile la nivel de circuit.

Cînd un client doreşte să se conecteze la un server, aplicaţia client se va conecta, mai întîi, la un proxy server SOCKS care se va conecta, apoi, la serverul de aplicaţii. Schimbul de date dintre client şi serverul de aplicaţii se va realiza prin intermediul serverului SOCKS.

Există două versiuni ale acestui protocol : SOCKSv4 şi SOCKSv5. Prima versiune îndeplineşte trei funcţii : lansează cererile de conexiune, stabileşte circuitele şi realizează schimbul de date între aplicaţii. Versiunea 5 adaugă la aceste facilităţi şi posibilitatea autentificării clientului.

Mai multe detalii puteţi afla la adresa http : //www.socks.permeo.com.

5. *Secure Shell (SSH)*

Dezvoltat de către SSH Communications Ltd, Secure Shell este o aplicaţie care permite accesarea unui calculator aflat la distanţă prin intermediul unei conexiuni securizate. Informaţiile transmise între cele două calculatoare sînt criptate şi pot fi comprimate. Clientul trebuie să se autentifice printr-o parolă sau cheie de criptare. Criptarea poate fi folosită şi pentru identificarea sistemului.

Există două variante ale acestui standard : SSH1 şi SSH2. Ambele variante oferă variante împotriva atacurilor de tip spoofing.

Pentru mai multe detalii vă recomandăm http : //www.employees.org/satch/ssh/ faq/ ssh-faq-1.html→ss1.1.

6. *Secure Sockets Layer (SSL)*

Probabil vi s-a întîmplat să accesaţi un site a cărui adresă era de forma „*https : //...*" în loc de varianta clasică. În termeni simpli, acest lucru înseamnă că sesiunea dintre browserul dumneavoastră şi serverul accesat este securizată.

SSL este un protocol de securitate dezvoltat iniţial de Netscape şi RSA Data Security. El realizează un canal privat de comunicaţie între două calculatoare asigurînd integritatea şi confidenţialitatea datelor, dar şi autentificarea partenerilor de dialog.

SSL are două componente :

- un protocol pentru transferul datelor (SSL Record Protocol) folosind chei predefinite şi combinaţii de autentificare ;
- un protocol pentru autentificarea iniţială a clienţilor şi transferul cheilor de criptare (SSL Handshake Protocol).

Mai multe detalii pot fi obţinute direct de la sursă : http : //developer.netscape. com/ docs/manuals/security/sslin/contents.htm.

1. Definit în RFC 1928, 1929.

7. *Virtual private networks (VPN)*

VPN reprezintă un mod de a conecta locații aflate la distanță (filiale, utilizatori mobili, clienți, furnizori etc.) într-o unică rețea virtuală, asigurîndu-se mecanisme de securitate.

Pentru a realiza un VPN se folosește un mediu public de transmisie - de exemplu, Internetul - în locul liniilor dedicate care sînt foarte scumpe sau „remote access" prin dial-up la mari distanțe geografice. Prin folosirea serviciilor unui așa-numit furnizor de servicii Internet (ISP - Internet Service Provider), se realizează foarte rapid conectarea la Internet. Pentru că acești ISP sînt foarte răspîndiți, se pot alege în funcție de zona geografică în care se află sediul central sau filialele companiei, asigurîndu-se pentru fiecare dintre acestea o conectare ieftină la Internet prin dial-up sau linie închiriată locală - în funcție de mărimea și necesitățile de comunicație ale biroului sau filialei respective. Spre exemplu, fiecare conectare la Internet prin dial-up implică doar costul unei convorbiri locale (cu ISP-ul local). Prin folosirea unor mecanisme de securitate se asigură confidențialitatea datelor. Se pot utiliza mecanisme de criptare a datelor vehiculate, ceea ce înseamnă că numai expeditorul care posedă cheia de criptare și destinatarul care posedă cheia de decriptare pot avea acces la date. De asemenea, prin mecanisme de autentificare, se poate asigura ca numai utilizatorii autorizați să aibă acces la informațiile confidențiale ale companiei. VPN creează așa-numitele tuneluri care străbat Internetul între sursa de date și destinație. Acest tunel este invizibil pentru utilizatorii din afara VPN ; în plus, toate datele care se transmit prin tuneluri sînt criptate. Fiecare utilizator din VPN este verificat și comparat cu baza de date existentă și i se aplică nivelul de securitate specific.

Virtual Private Network rezolvă cea mai stringentă problemă a Internetului : asigurarea confidențialității datelor prin criptarea și încapsularea datelor în timpul transmiterii. Datele sînt comprimate și apoi încapsulate pentru a ascunde adresa fiecărui pachet. Datele încapsulate sînt transmise printr-un tunel sigur care este inițializat la fiecare sesiune de transmisie date. Acest tunel se folosește pentru a transmite numai date din interiorul VPN. După inițializarea tunelului, utilizatorul care dorește să comunice este autentificat pe baza informațiilor introduse în baza de date a mecanismului central al VPN. O dată autentificat, utilizatorul are drept de acces la acele resurse din rețea la care a fost autorizat de către administratorul rețelei.

La capătul celălalt al tunelului - rețeaua locală a companiei - datele sînt autentificate, reasamblate și rutate către calculatorul din rețea căruia i-au fost destinate. Datele din tunel sînt inaccesibile altor utilizatori din Internet, eliminîndu-se astfel posibilitatea de interceptare a pachetelor de date.

12.3. Proiectarea unei rețele. Studiu de caz

1. *Ipoteze de lucru*

Dacă pînă în acest moment am prezentat aspectele generale cu privire la proiectarea unei rețele locale, a sosit momentul să vedem și cum stau lucrurile din punct de vedere practic. Vom lua ca exemplu dezvoltarea unei rețele de dimensiuni mici[1] (maximum 100 de utilizatori). În scenariul nostru trebuie să ținem cont de :

1. Cele medii se consideră că au 100-500 utilizatori, iar cele mari, peste 500.

- Bugetul de care dispune firma pentru acest proiect;
- Aplicaţiile care rulează sau care vor fi implementate într-un viitor apropiat;
- Toleranţa la cădere;
- Configuraţia;
- Managementul reţelei;
- Experienţa utilizatorilor şi evoluţia reţelei.

După cum spuneam la începutul acestui capitol, proiectarea unei reţele demarează cu etapa de identificare a aplicaţiilor ce vor fi folosite în firmă. De obicei, într-o astfel de reţea, aplicaţiile care rulează sînt relativ simple: procesoare de text, programe de calcul tabelar, e-mail, o aplicaţie client-server, Web.

Prin urmare, astfel de aplicaţii nu sînt consumatoare de lăţime de bandă, deoarece, în majoritatea timpului, utilizatorii lucrează cu fişiere de pe propriile staţii de lucru. Consumul de lăţime de bandă apare în momentul autentificării utilizatorilor sau cînd se deschid fişierele de pe server.

Dacă tot am ajuns la servere, se poate presupune că, în cele mai multe cazuri, serverele sînt Windows (de la NT la 2003 Server) sau Linux/Unix şi rulează un sigur protocol: TCP/IP. Reţelele care rulează doar un protocol sînt mai uşor de proiectat şi depanat în situaţia în care apar probleme. În eventualitatea în care se doreşte utilizarea unui router, acesta va putea fi unul mai ieftin care să ştie doar IP (nu va fi nevoie de un router multiprotocol).

Din punctul de vedere al resursei umane, vom întîlni unul sau doi administratori de reţea/ingineri de sistem. Se cuvine să amintim că în practica românească este obligatoriu să ai cunoştinţe despre sistemul de operare dacă te aventurezi pe tărîmul reţelelor. Administrarea unei reţele nu este încă văzută distinct faţă de sistemul de operare folosit, iar administratorul de reţea este în cele mai multe cazuri un fel de „medic generalist" care se pricepe mai mult la sistemul de operare decît la switch-urile/routerele din reţea.

Dacă ne întoarcem la aspectele cu care am început discuţia, putem trage cîteva concluzii:

- Din punctul de vedere al bugetului, într-o astfel de reţea echipamentele trebuie să coste cît mai puţin.
- Aplicaţiile care rulează pot partaja în cele mai multe cazuri lăţimea de bandă a reţelei. Pentru excepţii se va face apel la switch-uri.
- Pentru backbone este suficientă soluţia oferită de switch-uri.
- Configuraţia va fi stea extinsă.
- Cerinţele legate de management sînt minime. De obicei, administratorul rezolvă la faţa locului toate problemele.
- Creşterea previzionată pe termen mediu este de 25-50%.

Aici se cuvine să facem o scurtă precizare. Previzionarea dezvoltării reţelei este etapa cea mai dificilă din practică, după părerea noastră ca efect a cel puţin trei stări de fapt. Pe de o parte, administratorul de reţea se ocupă, după cum spuneam, mai mult de servere, iar pe de altă parte, în multe firme IT-ul este văzut ca un consumator de mari resurse financiare şi mai puţin producător de profit. În al treilea rînd, sînt multe situaţii în care mai întîi se alocă un buget pentru realizarea reţelei, iar la scurt timp se află şi care sînt aplicaţiile care trebuie obligatoriu să ruleze în reţea!

Așa stînd lucrurile, nu ne rămîne decît să enumerăm cerințele proiectului:

- 75 de utilizatori;
- un server pentru autentificare și fișiere. În viitor se vor mai adăuga două: unul pentru baze de date și unul pentru acces la Internet;
- 10 imprimante;
- mail intern;
- acces la Internet pentru anumiți utilizatori (Web, ftp, e-mail);
- un server Web.

2. *Identificarea cerințelor hardware – proiectarea fizică*

Conectica unei astfel de rețele nu implică resurse sofisticate, dar înainte de a ajunge la aceste componente, trebuie înțelese funcțiile pe care le îndeplinesc serverele și modul de amplasare a acestora. Dacă e să facem o clasificare a serverelor din punctul de vedere al utilizatorilor pe care îi deservesc, putem vorbi de servere organizaționale și servere pentru grupuri de lucru. Serverele organizaționale ar trebui să fie cele care oferă servicii tuturor utilizatorilor firmei: e-mail, www.

Cisco recomandă ca serverele organizaționale să fie amplasate în MDF (*Main Distribution Facility*) pentru a se evita ca traficul către acestea să traverseze și celelalte rețele. MDF este o sală în care va fi localizat nodul principal al rețelei firmei, amplasată de obicei cît mai aproape de locul în care se face legătura cu rețeaua externă.

Ideal ar fi ca serverele grupurilor de lucru să fie amplasate în IDF (*Intermediate Distribuiton Facility*) sau, altfel spus, cît mai aproape de utilizatorii care au nevoie de aplicațiile găzduite de aceste servere. În acest mod, traficul informațional va traversa infrastructura IDF-ului respectiv fără a mai afecta și alți utilizatori. Pentru a lega IDF-urile de MDF se recomandă folosirea unor switch-uri care să ofere o lățime de bandă de cel puțin 100Mbps.

Selecția și amplasarea echipamentelor reprezintă o decizie care trebuie să aibă la bază în primul rînd reducerea coliziunilor în rețea. Numărul broadcast-urilor devine excesiv în momentul în care există prea multe pachete-client ce necesită servicii sau prea multe pachete-server care anunță servicii, actualizări ale tabelelor ARP etc.

Pe măsură ce rețeaua se dezvoltă, incluzînd din ce în ce mai multe noduri pe același segment, șansa ca un astfel de nod să nu mai funcționeze este destul de mare: crește numărul coliziunilor. Chiar dacă acest fenomen este ceva normal în cazul Ethernet, un număr excesiv de coliziuni contribuie la reducerea lățimii de bandă. În majoritatea cazurilor, lățimea de bandă teoretică se reduce cu pînă la 40% din cauza coliziunilor. Soluția o reprezintă bineînțeles segmentarea.

Utilizatorii acestei rețele vor fi împărțiți în două categorii, în funcție de aplicațiile pe care le folosesc: *productivi* (cei care folosesc aplicații în mod constant, imprimă documente etc) și *administrativi* (folosesc calculatorul ocazional pentru mail sau tehnoredactare). Este nevoie de o astfel de clasificare pentru a putea oferi fiecărei categorii de utilizatori resursele exacte de care are nevoie.

La o primă vedere, rețeaua noastră va putea arăta ca în figura următoare, dacă luăm în calcul doar alocarea unui buget cît mai mic.

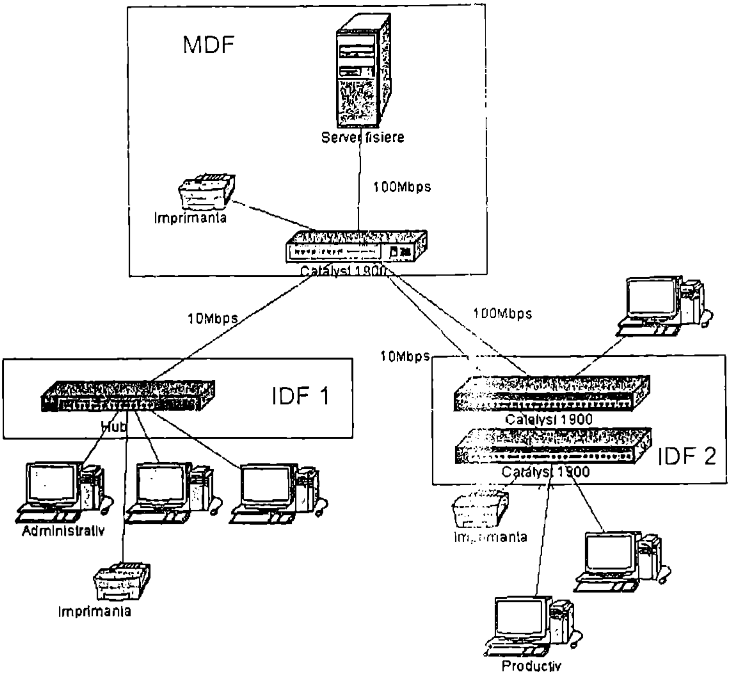


Figura 12.3.1. Structura unei reţele

Am folosit un hub cu porturi pe 10Mbps pentru a conecta utilizatorii din grupul *administrativ*, pentru că am considerat că aceştia nu au nevoie de mai mult pentru sarcinile curente. În plus, este şi mai ieftin decît un switch.

Pentru utilizatorii din grupul *productiv* am luat în calcul două legături: una pe 10Mbps şi cealaltă pe 100Mbps. Switch-urile din MDF şi IDF 1 sînt Catalyst 1900 şi, chiar dacă au cîte 24 porturi pe 10 Mbps, pentru lăţime de bandă mai mare nu dispun decît de două porturi pe 100 Mbps.

Reţeaua de mai sus nu ţine cont însă de dezvoltările viitoare: apariţia unor noi servere, creşterea numărului de utilizatori, accesul la Internet.

Dacă însă vom căuta să ţinem cont de toate aspectele enumerate la începutul scenariului şi vom aloca ceva mai multe resurse financiare, se impun cîteva schimbări. O soluţie ar fi ca switch-ul din MDF să fie unul cu mai multe porturi pe 100Mbps pentru a putea conecta cît mai multe servere sau switch-uri. În al doilea rînd, ca efect al acestei schimbări, backbone-ul reţelei interne trebuie să ofere şi el tot 100Mbps. Propunem deci ca switch-urile din IDF2 să fie din aceeaşi categorie, iar cel din IDF 1 să fie unul cu cel puţin 2 porturi pe 100Mbps, iar restul pe 10 Mbps. Dacă se doreşte economie în bugetul proiectului, se poate renunţa la switch-ul din IDF 1 şi este recomandabilă înlocuirea acestuia cu un hub.

Diagrama fizică a noii rețele ar putea arăta ca în fig. 12.3.2 :

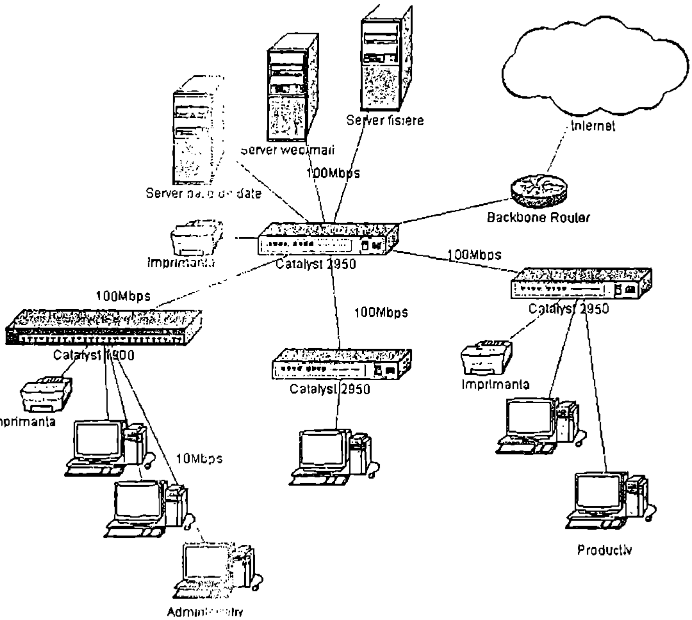


Figura 12.3.2. Diagrama fizică a rețelei

Nu am luat în calcul caracteristicile clădirii pentru care se realizează acest proiect.

3. *Proiectarea logică*

În proiectarea logică a rețelei trebuie să pornim de la ceea ce se dorește din punctul de vedere al securității sau al accesului. Dacă nu se impun restricții se poate opta pentru varianta amplasării tuturor dispozitivelor într-o singură rețea. După cum se observă și din diagrama anterioară (există o singură legătură între router și switch), aceasta este și varianta pe care am ales-o.

Adresarea

Pentru o rețea cu pînă la 100 de utilizatori vom folosi o rețea din clasa C : 192.168.1.0/24.

Pentru a fi mai ușor de administrat, vom rezerva primele 10 adrese pentru servere (192.168.1.1-192.168.1.10), următoarele 20 pentru imprimante (192.168.1.11-192. 168.1.30), ultimele 5 pentru router (192.168.1.250-192.168.1.254), iar celelalte pentru stațiile utilizatorilor. Pentru a decide maniera de alocare a acestor adrese trebuie să identificăm care este numărul exact de utilizatori conectați la rețea și care este rata schimbărilor (adăugare, mutare sau redenumire a unor dispozitive).

Tabelul 12.3.1. Exemplu Foaie de lucru

Proiect: Reţea "ABC" SRL								
Reţea	192.	168.	1	X		**Subnet mask**	255.255.255.0	
Localizare	*Parter clădire*					**DNS**	x.x.x.x	
Adresare								
	192.	168	1.	250	Default gateway pentru retea/subretea			
	192.	168	1.	31-249	Rezervate utilizatorilor			
	192.	168.	1.	1-10	Rezervate serverelor			
	192.	168.	1.	11-30	Rezervate imprimantelor			
	192	168.	1	250-254	Rezervate routerului			
Utilizare estimată şi Istoric								
La această dată sînt 75 de utilizatori. Se estimează o creştere de 10% în următorul an								
Configuraţia VLAN-urilor								
Nu s-au folosit încă								
Hardware								
	Conectică retea				Hub	Nu		
					Switch	DA	2*Catalyst2950 1 Catalyst 1900	24*100BaseTX 2 module Gigabit 2*100BaseTX 12*10BaseT
					Router	DA	Catalyst 2600	2*FastEthernet 2*Serial

Într-o firmă cu 10-20 de utilizatori, este puțin probabil să existe un angajat care să se ocupe doar de administrarea rețelei. În acest caz, alocarea statică a adreselor reprezintă soluția optimă.

Dacă, în schimb, pentru aceeași situație se preconizează creșterea numărului de utilizatori, schimbări dese în amplasarea echipamentelor, instalarea unui server DHCP poate reprezenta soluția problemei, chiar dacă pentru aceasta este nevoie de cunoștințe mai de specialitate.

Management

Facilitățile de administrare a unei rețele nu trebuie corelate cu dimensiunea acesteia. Singurul element care poate afecta acest aspect este bugetul disponibil pentru proiect. În scenariul nostru am ales dispozitive de rețea ce pot fi administrate (cu management). Cînd resursele financiare permit, este recomandabil să existe în rețea și o stație dedicată managementului acesteia. Pentru situațiile cînd acest lucru nu este posibil, se poate apela la soluția bazată pe Web (dispozitivul poate fi accesat prin intermediul browserului de oriunde din rețea).

Rezolvarea numelor - DNS

Dacă în rețea serviciile cerute de clienți serverelor implică existența unei relații între aceste servicii și resursele hard, trebuie ca fiecare dintre clienți să poată rezolva numele asociat acelei resurse (*domain name*). Această problemă are două soluții : folosirea unui fișier pentru host-uri sau configurarea unui DNS, dacă rețeaua este mai complexă (peste 70-80 de clienți). Dacă se va ține cont de dezvoltările viitoare din organizație, este recomandabil să se gîndească o structură ierarhizată a numelor încă de la începutul proiectului, pentru a se evita reproiectarea acestuia mai tîrziu.

Conectarea la Internet

În scenariul nostru am folosit adrese IP private (nerutabile) din motive de securitate. Aceasta este soluția pe care o adoptă cele mai multe firme în practică. Pentru conexiunea externă firmele achiziționează de la furnizorii de servicii un număr limitat de adrese sau chiar un interval întreg, urmînd ca în interiorul rețelei să folosească adrese private. Pentru conversia acestora din urmă în adrese rutabile se configurează NAT pe un server sau routerul organizației.

CAPITOLUL 13

Instalarea şi configurarea logică a unei reţele locale

În proiectarea oricărei reţele trebuie să se ţină seama, pe lîngă alegerea celei mai bune topologii, şi de alegerea celui mai potrivit sistem de operare.

Decizia de alegere a unui sistem de operare trebuie luată după o analiză atentă a necesităţilor şi a resurselor disponibile. Principalii factori care pot influenţa decizia de a alege un sistem de operare pot fi :

a) **Compatibilitatea aplicaţiilor care vor fi utilizate cu sistemul de operare.** Majoritatea aplicaţiilor existente pe piaţă sînt dedicate unui sistem de operare, rularea acestora pe alte sisteme de operare fiind practic imposibilă.

b) **Preţul** este un subiect căruia trebuie să i se acorde o importanţă deosebită, pentru că utilizarea unui sistem de operare fără plata licenţei pentru acesta se sancţionează conform legilor în vigoare. Salvarea vine de la sistemele de operare de tip Linux, care sînt gratuite, putînd fi utilizate în orice instituţie, în desfăşurarea oricărei activităţi legale. De asemenea, o dată cu kit-ul de instalare a sistemului Linux, pot fi livrate şi sursele acestuia care pot fi modificate şi compilate.

c) **Resursele fizice existente.** Fiecare sistem de operare are specificată în documentaţia sa resursele fizice minime necesare rulării acestuia. Nu trebuie însă să ne bazăm numai pe acest lucru ! În decursul utilizării, de cele mai multe ori, se doreşte instalarea de aplicaţii noi, care au nevoie, la rîndul lor, de resurse fizice, ceea ce poate duce la veşnica dilemă : *Nu instalez aplicaţia sau efectuez un update ? !*

Anumite sisteme de operare pretind resurse mai puţine prin specificaţii, dar scade şi calitatea sistemului instalat, nu atît din punctul de vedere al siguranţei, stabilităţii sau fiabilităţii, ci din punctul de vedere al interfeţei cu utilizatorul.

O reţea trebuie să conţină cel puţin un server. Şi dacă am ajuns aici, trebuie să lămurim că nu este obligatoriu ca serverul să fie definit ca cel mai performant (din punct de vedere fizic) calculator din reţea, şi nici să scriem „cu pixu'" pe el *Server* ca să ştim să-l deosebim de celelalte calculatoare (staţii de lucru). Serverul trebuie să îndeplinească anumite roluri (server de autentificare, de baze de date, de backup, de aplicaţii, de fişiere, de Web, de e-mail, de monitorizare) care-i conferă un statut special faţă de celelalte staţii de lucru din reţea, aceste servicii necesitînd în schimb o serie de resurse fizice suplimentare. Îmbunătăţirea unei staţii de lucru obişnuite prin adăugarea de memorii nu constituie cea mai bună soluţie, serverele dedicate avînd o arhitectură mai robustă, însăşi funcţionarea permanentă a acestora necesitînd prezenţa unor ventilatoare suplimentare !

d) **Uşurinţa în utilizare.** Acest aspect poate deveni o sabie cu două tăişuri pentru că se referă direct la utilizatorii sistemului respectiv. Puţini sînt cunoscătorii sistemului de operare Linux, chiar dacă acesta este gratis, economiile din banii de licenţă se „topesc" în pregătirea cursanţilor sau în achiziţia de materiale pentru instruire. Situaţia tristă apare, de obicei, cînd angajaţii nu cunosc nici o altă versiune de sistem de operare de pe piaţă. Balanţa se înclină, de cele mai multe ori, în favoarea părţii care este influenţată cel mai mult de ceilalţi factori.

Trebuie menţionat rolul deosebit în domeniul pregătirii viitorilor angajaţi ai instituţiilor de învăţămînt. Un cursant, dacă învaţă specificul unei anumite aplicaţii, se va orienta către instituţiile care-i pot oferi mediul de lucru pe care-l cunoaşte.

e) **Asigurarea serviciilor de bază ale reţelei** prin implementarea şi asigurarea comunicării, autentificării, securităţii şi siguranţei în utilizare ar trebui, chiar dacă ordinea n-o specifică, să fie unul dintre cele mai importante motive în alegerea un sistem de operare sau altul. Fiecare sistem de operare îşi îndeplineşte foarte bine funcţiile pentru care a fost creat (dacă este bine configurat), dar fiecare în felul său, recomandabilă fiind combinarea prin completare a lor, puţine fiind la ora actuală reţelele formate dintr-un singur sistem de operare.

13.1. Care este cel mai bun sistem de operare? !

Aceasta este, probabil una dintre cele mai vehiculate întrebări în lumea IT, dar, în acelaşi timp, şi sursa expansiunilor şi îmbunătăţirilor continue ale sistemelor de operare. Un răspuns exact nu poate da nimeni, cel mai corect ar fi să se spună că *cel mai bun sistem de operare este cel pe care-l cunoşti*, fără a exclude de aici ideea că *depinde pentru ce îl foloseşti*! De multe ori se întîmplă să nu găseşti în sistemul de operare pe care-l cunoşti soluţia cea mai viabilă pentru rezolvarea anumitei probleme... *Te apuci de învăţat sau suni un prieten ? !*

Şi, cum se poartă diletantismul politic, o să răspund în rîndurile următoare la o cu totul altă întrebare: *Care este cel mai utilizat sistem de operare în prezent ?*

Pornind de la ideea că Internetul este definit ca o reţea de reţele şi orice reţea care este conectată la Internet reprezintă o parte componentă a acestuia, am ales varianta căutării răspunsului la întrebarea anterioară, alături de noi, adică în cele mai variate locuri ale reţelei Internet.

Ca o primă idee, la ora actuală sînt înregistrate în mod oficial 30.640.114[1] de domenii pe Internet, din care ne putem extrage informaţia din cele mai inimaginabile domenii. În acest caz, găsirea informaţiei de care ai nevoie este comparabilă cu găsirea peştişorului de aur într-un ocean.

Desigur, acest pasaj nu trebuie să se constituie într-un alt factor de alegere a unui anumit sistem de operare, ci trebuie privit doar ca o analiză la rece a ceea ce ne spun cifrele. Am analizat în acest scop log-urile de acces către 10 site-uri Web din ţara noastră şi 21 de site-uri comerciale, educaţionale, guvernamentale şi militare din SUA, Canada, Marea Britanie, Italia şi Elveţia, totalizînd 329.547.274 de vizitatori unici total pentru anul 2002.

1. Pentru corectitudinea cifrei respective, la momentul în care consultaţi acest material, vizitaţi site-ul http://www.domainstats.com/, cunoscut fiind faptul că reţeaua Internet se află într-o continuă dezvoltare exponenţială.

Rezultatele acestei analize sînt prezentate în tabelul 13.1.1 :

Tabelul 13.1.1. O analiză a celor mai utilizate sisteme de operare ca suport pentru browserele de Internet

Site-uri din România		Site-uri din Europa de Vest şi America de Nord	
Platforma	**Procent**	**Platforma**	**Procent**
Windows 98	50.56%	Windows 98	33.19%
Windows 2000	17.71%	Windows 2000	24.47%
Windows NT	12.98%	Windows ME	9.94%
Windows 95	6.00%	Windows NT	9.33%
Windows XP	5.54%	Altele	9.16%
Windows ME	5.16%	Windows 95	6.30%
Altele	0.86%	Macintosh PowerPC	3.35%
Unix	0.60%	Windows XP	3.06%
Macintosh	0.29%	Linux	0.42%
Linux	0.28%	WebTV	0.25%
OS/2	0.01%	SunOS	0.18%
		Macintosh	0.10%
		Sonstiges	0.10%
		Unix	0.08%
		Windows 3.x	0.04%
		OS/2	0.00%
Total vizite	**2.969.714**	**Total vizitatori**	**329.547.274**

Sursa : pentru site-urile din România am cules informaţii de pe site-urile www.trafic.ro, www.grafstat.ro şi o serie de site-uri din reţeaua RoEduNet, iar pentru site-urile din afară, informaţiile au fost preluate direct de pe site-urile accesate. S-au ales pentru analiză doar site-urile care au cel puţin 50.000 de vizitatori unici pentru perioada studiată.

Datele din tabelul 13.1.2 sînt discutabile, pentru că site-urile din România n-au fost accesate numai de calculatoare din România, dar procentul ridicat de vizitatori din România ne duce la ideea, nu tocmai corectă, că din cei 313.584 de vizitatori unici identificaţi ca fiind din România, 50,56% folosesc sistemul de operare Windows 98, adică, putem deduce că, sistemul de operare Windows 98, este utilizat de aproximativ 50% dintre calculatoarele din România conectate la Internet.

După cum se observă şi pe site-urile din afara ţării noastre se înregistrează o dominare a sistemului de operare Windows 98. Este oare acesta cel mai bun sistem de operare ? ! Desigur că cei mai mulţi dintre cititori vor răspunde negativ la această întrebare. Mulţi alţii vor răspunde afirmativ. Singurul răspuns pe care-l pot da este : *Depinde !* Depinde la ce este folosit.

Tabelul 13.1.2. Top 13. Vizitatori, pe țări, care accesează site-uri din România

Rețea	Vizitatori	Procent
Romania (ro)	313.584	91.36%
Statele Unite (us)	22.118	6.44%
Moldova (md)	2.504	0.73%
Germania (de)	1.507	0.44%
Canada (ca)	806	0.23%
Israel (il)	792	0.23%
Austria (at)	497	0.14%
Franta (fr)	447	0.13%
Portugalia (pt)	352	0.10%
Finlanda (fi)	278	0.08%
Irlanda (ie)	180	0.05%
Marea Britanie (uk)	109	0.03%
Olanda (nl)	49	0.01%
Total vizitatori unici	**343.223**	**100%**

Sursa : http ://www.grafstat.ro/.

Într-o altă statistică, de această dată mult mai veche din păcate, plasează sisten operare Linux în topuri (tabelul 13.1.3).

Tabelul 13.1.3. Cele mai utilizate sisteme de operare folosite în România pentru găzduirea site-urilor Web.

Sistem de operare al serverului Web	Număr servere interogate	%
Linux	1645	59.7
Windows 95/98/NT	713	25.9
Solaris/SunOS	228	8.3
BSD Family	31	1.1
IRIX	28	1.0
Mac/Apple	23	0.8
AIX	11	0.4
SCO Unix	11	0.4
Digital Unix	9	0.3
HPUX	9	0.3
Novell Netware	9	0.3
Total site-uri testate	**2717**	**98.6**

Sursa : http ://leb.net/hzo/ioscount/data/r.9904.ro.txt, Aprilie, 1999.

Deci este mai bun sistemul de operare Linux? ! Acelaşi răspuns: *Depinde !*

Acest mister poate fi cît de cît elucidat, apelînd la argumentele utilizatorilor reţelei Usenet[1] :

- Windows este foarte uşor de instalat şi utilizat, pe cînd Linux necesită o configurare amănunţită înainte de a putea fi rulat la performanţe maxime. Windows este pentru toată lumea, Linux pentru foarte puţini.
- Linux este un sistem de operare care permite o configurare la nivel foarte ridicat, asigurînd o mult mai bună transparenţă a nucleului său, dînd astfel posibilitatea înţelegerii a ceea ce se întîmplă în interiorul calculatorului.
- Există mai multe aplicaţii pentru Windows. Windows recunoaşte şi poate lucra cu majoritatea echipamentelor hardware existente, pentru Linux existînd încă o serie de incompatibilităţi.
- Linux-ul este gratuit. Toate aplicaţii distribuite prin licenţierea Open Source includ codul sursă, fapt ce previne downloadarea şi rularea de aplicaţii pirat.
- Softul gratuit şi în special aplicaţiile pentru Linux sînt de cele mai multe ori puse la dispoziţie în versiunea Beta sau *work in progress*. Salutară în acest scop este iniţiativa unor corporaţii de a nu folosi software pe platforme Linux, pentru că acestea nu constituie o garanţie a performanţelor şi a securităţii în rulare.
- Windows-ul este ţinta principală a viruşilor; la instalare sau ulterior se creează şi se instalează o serie de fişiere şi aplicaţii care nu sînt utilizabile de multe calculatoare, creînd o stare de confuzie utilizatorilor. Totodată este un produs de monopol, concentrat în special pe cucerirea pieţei sistemelor de operare, nu pe îmbunătăţirea programelor sale.

N-am amintit aici de sistemul de operare MacOS, el fiind dedicat în special aplicaţiilor multi-media, parte minoră în majoritatea sistemelor informaţionale.

Mergînd pe principiul că cel mai bun sistem de operare este cel pe care-l cunoşti, o să prezentăm în continuare cîteva dintre facilităţile sistemului de operare Windows 2000, cu exemplificare pe o reţea locală. În discuţiile contradictorii Linux/Windows, care nu sunt puţine, se vorbeşte despre incapacitatea sistemului de operare Windows de a-şi automatiza activităţile prin crearea de script-uri. Prezentăm în partea finală a acestui capitol cîteva exemple de script-uri necesare instalării şi configurării unei reţele pur Windows.

Totodată, beneficiind de peste 400 de staţii de lucru, 12 servere dedicate şi peste 9000 de utilizatori, un contract MSDN Academic Alliance, putem spune că am reuşit să testăm, să studiem şi să implementăm cele mai importante facilităţi ale sistemului de operare Windows.

Materialul pe care-l prezentăm în continuare este fundamentat pe schema de reţea prezentată în fig. 13.1.2.

1. Computers&Internet, http://computers.alluneed2know.net/.

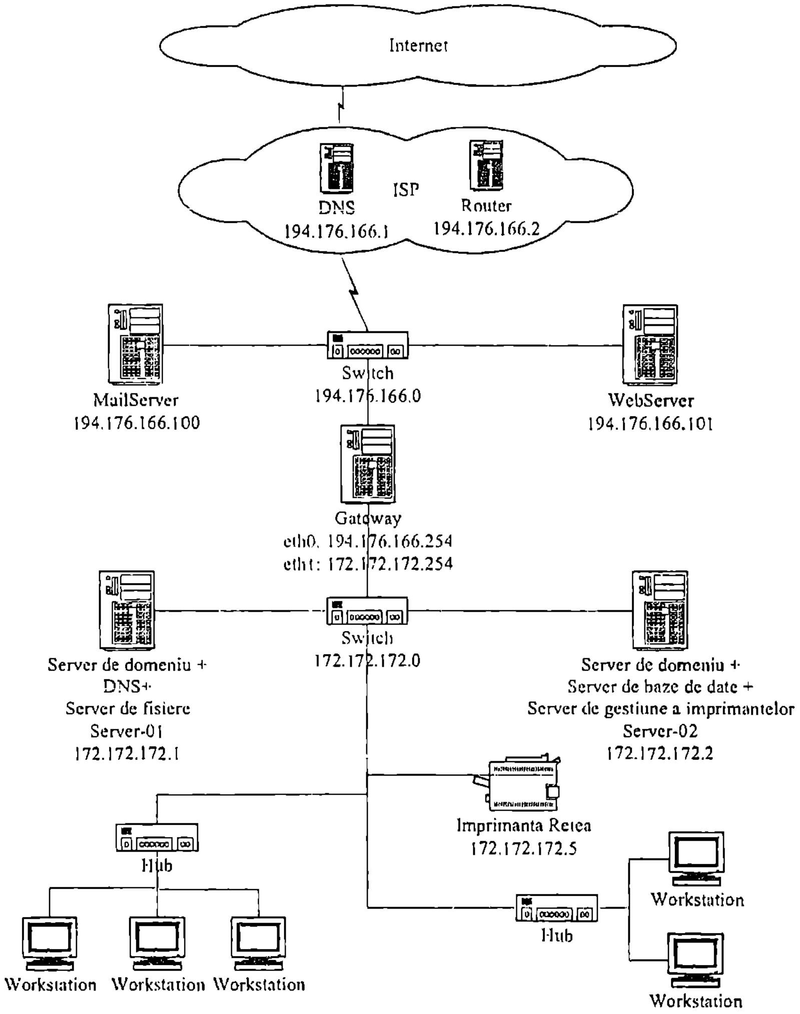


Figura 13.1.2. Structura unei rețele

13.2. Instalarea Windows 2000 Server

Nu de puține ori se spune că Windows este un mare consumator de resurse fizice. Dar cei care cunosc cît de cît Linux, pot recunoaște că orice interfață grafică instalată necesită la fel de multe resurse fizice ca cele necesare unui sistem.

Tabelul 13.2.1. Cerinţe fizice minime
pentru instalarea Windows 2000

Componentă	Specificaţiile Microsoft	Cerinţe minime reale*
Procesor	133 MHz Pentium sau superior	300 MHz Pentium II sau superior
Memorie RAM	• 32MB minim ; 64MB recomandat pentru staţii • 128MB minim ; 256 recomandat pentru servere	Mai mult de 96MB
Spaţiu pe disc	2GB, cu 1GB liber	2-4GB
Video	VGA sau mai bun	SVGA
Accesorii	Tastatură şi mouse sau alte dispozitive care să înlocuiască mouse-ul.	
Pentru instalarea de pe CD	Unitate de CD-ROM, 12x sau mai rapidă. Dacă sistemul d-voastră nu permite startarea (bootarea) de pe CD, aveţi nevoie de o unitate de citire a dischetelor.	
Pentru instalarea prin reţea	Una sau mai multe adaptoare de reţea (network card) precum şi infrastructura de comunicaţii : cabluri şi alte dispozitive.	

*) Concluzii la care s-a ajuns în urma unor discuţii pe forumuri specializate.

În continuare, vom parcurge pas cu pas etapele instalării sistemului de operare Windows 2000 Server.

1. *Instalarea în mod text*

Pasul 1 – Bootarea

În cerinţele minime solicitate de sistemul de operare Windows 2000 Server se specifică şi necesitatea existenţei unui CD-ROM.

În unitatea de CD-ROM se introduce CD-ul de instalare cu kit-ul de Windows 2000 Server care în mod normal este *bootabil* (sistemul de operare se lansează de pe CD). O condiţie pentru declanşarea operaţiunii de bootare de pe CD este să aveţi activată opţiunea respectivă din BIOS.

După ce apăsaţi o tastă, se lansează în execuţie aplicaţia *Setup* care în faza iniţială, încarcă fişierele de configurare (drivere) a diferitelor dispozitive hardware esenţiale continuării instalării.

Pasul 2 – Mesajul de întîmpinare

Prima intervenţie este alegerea operaţiunii pe care doriţi să o efectuaţi :

- *instalarea sistemului de operare.* Instalarea unui nou sistem de operare pe calculatorul curent (apăsaţi tasta **Enter** ; menţionăm că în această etapă se lucrează numai cu tastatura) ;
- *repararea instalării.* În cazul în care aveţi deja instalat sistemul de operare Windows 2000 Server, această opţiune este foarte bună în cazurile mai puţin fericite cînd sistemul a suferit anumite disfuncţionalităţi (apăsaţi tasta R) ;
- *ieşirea din aplicaţia Setup* în cazul în care aţi ajuns întîmplător sau din greşeală în această aplicaţie (apăsaţi tasta F3).

În cazul nostru vom apăsa cu încredere tasta Enter, urmată de un mesaj ceva mai consistent printre rîndurile căruia putem citi informații despre faptul că suportul nostru de stocare s-ar putea să fie nou sau toate datele de pe acesta au fost șterse. O problemă poate apărea în cazul în care pe același sistem de calcul este instalat un sistem de operare incompatibil cu Windows 2000.

Dacă sînteți siguri că aceste informații sînt corecte, puteți continua operațiunea de instalare apăsînd tasta C, cu riscul de a pierde toate informațiile de pe discul pe care veți realiza instalarea sau de a afecta un alt sistem de operare instalat anterior.

Recomandarea noastră este să instalați sistemul de operare pentru server pe o stație formatată și dedicată viitoarelor funcții pe care le va găzdui acesta.

Continuarea prin apăsarea tastei C aduce cu sine acceptarea licenței și condițiilor de utilizare a soft-ului. În această secțiune aveți două posibilități:

- *acceptarea licenței* (apăsați tasta **F8**), ceea ce vă permite continuarea instalării;
- *neacceptarea condițiilor licenței* (apăsarea tastei **Esc**), ceea ce duce automat la terminarea instalării.

Pasul 3 – Crearea partițiilor

Aceasta este o etapă importantă în stabilirea și configurarea viitoarelor partiții care vor fi utilizate pe server. În fig. 13.2.1. se observă că sistemul nostru are 3 discuri, și nici o partiție configurată.

Crearea unei noi partiții se poate realiza selectînd unul dintre cele 3 discuri și apăsarea tastei C (*To create a partition*). Instalarea poate continua însă și fără crearea în prealabil a unei partiții prin apăsarea tastei Enter (*To set up*). Dacă aveți deja partiții configurate pe discul sau discurile d-voastră, le puteți șterge prin selectarea lor cu săgeți și apăsarea tastei **D** (*To delete the selected partition*).

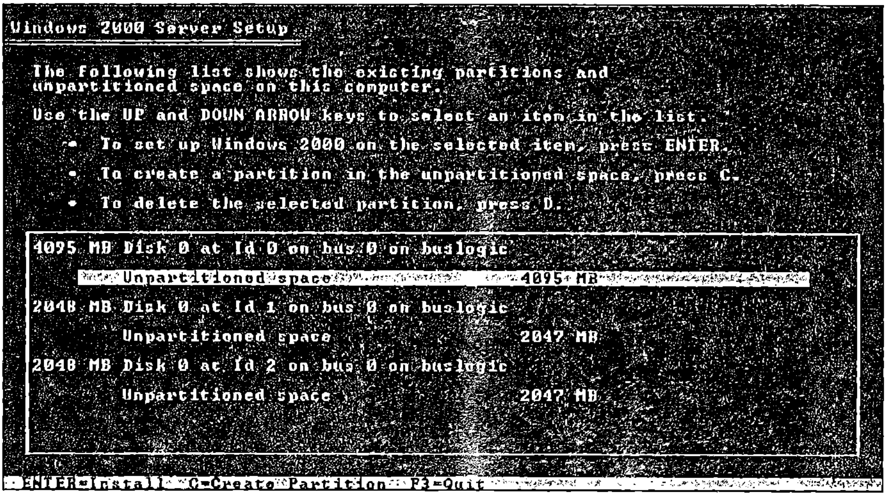


Figura 13.2.1. Alegerea discului pe care se realizează instalarea; crearea partițiilor

Numărul maxim de partiţii care pot fi create este limitat doar de dimensiunea discului/discurilor pe care le aveţi, ţinînd cont că dimensiunea minimă a unei partiţii este de 8 Mb. Numărul partiţiilor vizibile din Windows Explorer este limitat de numărul literelor din alfabet, excluzînd literele A, B, şi cea aferentă unităţii de CD-ROM.

Remarcă:	Este foarte posibil ca numărul maxim de partiţii configurabile pe un sistem Windows 2000 Server să se oprească în jurul valorii 256, dar se pare că răbdarea ne-a fost pusă greu la încercare de ambiţia sistemului de operare de a rezista la peste 180 de partiţii!

Creăm aşadar o partiţie pe primul disc, dimensiunea acesteia fiind de 1500 Mb, prin apăsarea tastei **C**, introducerea valorii *1500* în dreptul opţiunii *Create partition of size (in MB)*, şi confirmarea prin apăsarea tastei **Enter** (*Create*). Implicit, litera noii partiţii este *C:*, iar eticheta din dreptul partiţiei: *New (Unformated)* ne anunţă că următoarea etapă va fi aceea de ştergere a tuturor informaţiilor de pe partiţia respectivă (formatare). Apăsăm **Enter** (Install) trecînd la pasul următor.

Crearea celorlalte partiţii o vom detalia în capitolul „Configurare".

Pasul 4 - Formatarea partiţiilor

Din cele 2 opţiuni:

- Formatarea partiţiei utilizînd sistemul de fişiere *NTFS* şi
- Formatarea partiţiei utilizînd sistemul de fişiere *FAT*,

vă recomandăm cu căldură a doua variantă, sistemul de fişiere NTFS asigurînd suportul de securitate pentru fişiere şi directoare la nivel de utilizator sau grupuri de utilizatori!

Formatarea poate dura în funcţie de dimensiunea partiţiei create şi a vitezei de citire a discului între 1 şi 5 minute, urmată automat de etapele de verificare a discului contra erorilor fizice şi copiere a fişierelor pe disc de pe CD.

Cazuri speciale:

- Dacă doriţi instalarea pe un calculator pe care planificaţi să instalaţi şi alt sistem de operare care nu suportă NTFS, instalaţi Windows 2000 pe o partiţie secundară, de exemplu D:, şi formataţi discul C: utilizînd sistemul de fişiere FAT.
- Nu recomandăm instalarea W2k Server fără o formatare a partiţiei pe care se instalează acesta.

După terminarea copierii fişierelor, urmează o etapă scurtă de iniţializare şi verificare a instalării şi prima repornire (rebootare) a sistemului, care se efectuează automat în termen de 15 secunde sau poate fi „stimulată" prin apăsarea tastei *Enter*.

După repornire se trece în etape de configurare în mod grafic (GUI Mode).

2. *Instalarea în mod grafic*

După prima fereastră de Bun venit (Welcome Screen), care conţine un buton **Next** a cărui acţionare este opţională (trecerea se realizează automat după 30 de secunde), se trece la pasul nr. 5.

Pasul 5 – Iniţializarea şi instalarea dispozitivelor fizice

Detectarea resurselor hardware ale sistemului se realizează automat, Windows 2000 beneficiind de un suport plug-and-play destul de ridicat. La aproximativ jumătatea instalării, ecranul monitorului d-voastră o să clipească de cîteva ori. Nu intraţi în panică, pentru că acest lucru se datorează iniţializării adaptorului grafic.

Pasul 6 – Personalizarea opţiunilor pentru regiunea geografică şi tastatură

Pentru a instala o tastatură românească trebuie să activaţi de la setările locale (*local settings*) apăsînd butonul **Customize** (cel de sus), iar în fereastra *Regional Options*, tab-ul **General**, activaţi opţiunea **Central European**, apoi butonul **OK**.

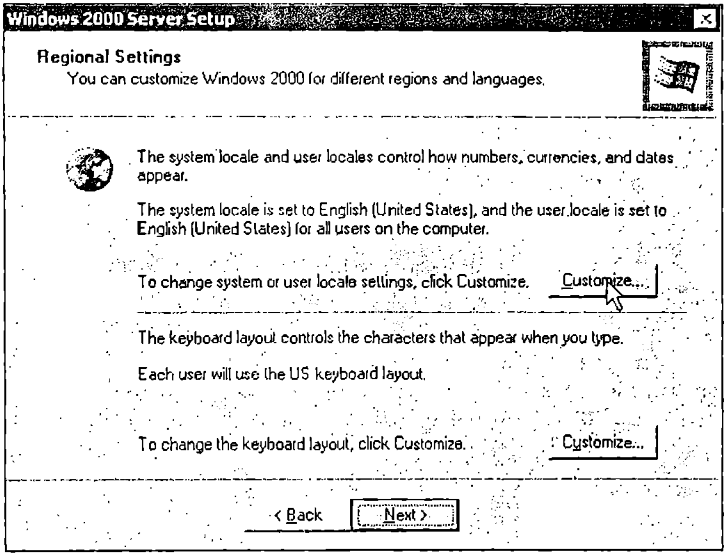


Figura 13.2.2. Personalizarea regiunii geografice şi tastaturii

Apăsaţi apoi butonul **Customize** din dreptul opţiunii *To change the keyboard layout*, şi din fereastra *Regional Options* apăsaţi butonul **Add**; din lista *Input Locals* alegeţi opţiunea *Romanian*, click pe OK.

În mod implicit, cînd se lucrează, mai este necesară schimbarea tastaturii din română în engleză şi invers. Schimbarea se realizează prin combinaţia de taste <Alt+Shift>, în mod implicit, dar această combinaţie poate fi schimbată cu una mai rapidă apăsînd pe butonul *Change Key Sequence* şi se poate schimba combinaţia de taste în <Ctrl+Shift>, după care se acţionează butonul OK. Închideţi această fereastră prin butonul OK şi treceţi la pasul următor apăsînd butonul **Next**.

Pasul 7 – Personalizarea software-ului

În această etapă se introduc informaţii generale despre numele celui care a achiziţionat licenţa pentru sistemul de operare (completaţi căsuţa *Name*) şi numele organizaţiei (căsuţa *Organization*).

Acţionarea butonului **Next** vă aduce în faţa ferestrei de introducere a cheii de verificare a autenticităţii software-ului pe care-l folosiţi. Dacă nu aveţi un astfel de număr, instalarea se poate opri aici. Utilizarea altui număr serial decît cel oferit de licenţa pe care aţi achiziţionat-o reprezintă o fraudă şi se pedepseşte conform legilor în vigoare.

Pasul 8 - Modul de licenţiere

Windows 2000 server suportă 2 tipuri de licenţiere:

- *per server*, pentru stabilirea de către server a numărului de conexiuni concurente;
- *per seat*, în care fiecare staţie de lucru din domeniu are propriul său C.A.L. (*Client Access License*) achiziţionat o dată cu sistemul de calcul.

Şi totuşi, prima variantă pare a fi mai valabilă pentru că într-o reţea pot exista sisteme hibride cu diferite sisteme de operare care ar putea să nu aibă un C.A.L.

În modul de licenţiere *per server*, numărul de conexiuni este dat de numărul clienţilor care a fost achiziţionat o dată cu sistemul de operare. Acest număr poate fi schimbat şi se stabileşte în funcţie de necesităţile fiecărei reţele: de exemplu, dacă aveţi o reţea de 50 de calculatoare, numărul optim de conexiuni simultane poate fi 100 sau 150, numărul minim fiind de 50.

Pasul 9 - Numele calculatorului şi parola de administrator

În această etapă trebuie să se stabilească numele calculatorului, care trebuie să fie diferit de alte denumiri din reţea pentru a nu intra în conflict. Numele implicit este generat automat (de exemplu: FEAA-T0306UG01D), dar pentru o mai bună recunoaştere în reţea o să-l schimbăm cu o denumire sugestivă mai uşor de reţinut: *Server-01*. Nu puteţi folosi în denumirea calculatoarelor o serie de caractere speciale sau caractere româneşti, aşa că vă recomandăm să folosiţi doar caractere, litere şi underscore (linie jos) sau cratimă.

Parola utilizatorului Administrator trebuie să reprezinte o combinaţie de caractere: litere, cifre sau caractere speciale în aşa fel încît să nu depăşească 127 caractere şi să nu se bazeze pe cuvinte uzuale, date de naştere sau numărul de la maşină. Utilizarea caracterului spaţiu sau a caracterelor speciale (numere în combinaţie cu tasta **ALT** din stînga tastaturii) face dintr-o parolă una mai puternică care ar lua foarte mult timp programelor de decriptare a parolei să o descopere. După cum v-aţi imaginat, parola nu este vizibilă, dar în exemplul nostru, vom folosi o parolă formată din 6 caractere asterix (*). Dacă în căsuţa de confirmare a parolei nu aţi introdus aceeaşi parolă, nu puteţi trece la pasul următor.

Pasul 10 - Stabilirea componentelor care vor fi instalate

Componentele pe care doriţi să le instalaţi sînt dependente de necesităţile viitorului server. Din această fereastră anumite componente au şi subcomponente pe care le puteţi vizualiza apăsînd butonul **Details**. Vă oferim, în continuare, o configuraţie minimă necesară unui viitor server de domeniu.

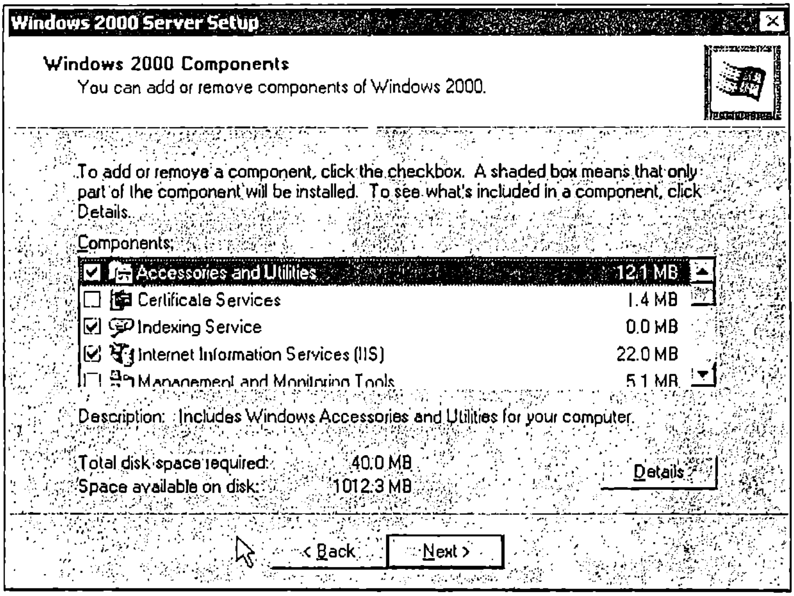


Figura 13.2.3. Alegerea componentelor care vor fi instalate

Din subcomponentele categoriei *Accessories and Utilities* :

- dezactivaţi *Accessibility Wizard*, dacă persoana care va administra serverul nu are probleme de natură fizică;
- din *Communications*, dezactivaţi *Phone Dialer*, dacă nu vă conectaţi la Internet de pe acest server printr-un modem;
- *Games*... de obicei noi le dezactivăm, dar... dacă preconizaţi că vă veţi plictisi la serviciu puteţi să le lăsaţi. Daţi-mi voie să dezactivez în configuraţia mea jocurile *Freecell* şi *Minisweeper* pentru că nu le-am înţeles niciodată;
- dacă aveţi placă de sunet pe server, puteţi să păstraţi componentele *Multimedia*, dar... un server de obicei se instalează, se configurează, se pune într-un dulap sub cheie şi se mai verifică din cînd în cînd. Opinia noastră este că „serverul e server, nu staţie de jocuri sau pentru ascultat muzică"! Aşadar, am dezactivat deja opţiunea *Multimedia*.

Aceste componente pot fi instalate sau dezinstalate ulterior.

Certificate Service reprezintă suportul pentru aplicaţiile care utilizează chei publice de securitate, permiţînd instalarea şi configurarea certificatelor de autoritate (*Certificate Authority*). Nu instalăm această componentă în această etapă.

Indexing Service reprezintă serviciul care face disponibilă căutarea rapidă a fişierelor bazată pe textul din conţinutul acestora. Acest serviciu este însă unul care ocupă şi foloseşte sistematic destul de multe resurse logice, mai ales în cazul serverelor de fişiere. Dezactivăm în această etapă şi serviciul respectiv.

Internet Information Service (IIS) reprezintă serviciul care se instalează şi se configurează pentru a putea pune la dispoziţie fişiere via Web, utilizînd serviciul HTTP. **Atenţie**: nu instalaţi acest serviciu pe serverele de domeniu, pentru că accesul prin HTTP reprezintă un risc de securitate suplimentar într-o reţea de calculatoare.

Dacă serverul pe care instalaţi nu este server de domeniu, puteţi instala acest serviciu, dar o să intrăm puţin în detaliile acestuia:

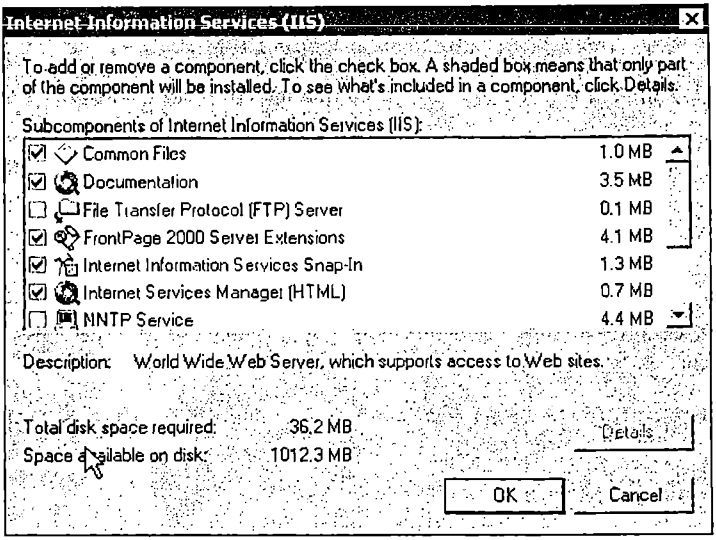


Figura 13.2.4. Prezentarea detaliată a componentelor serviciului IIS

- *Serviciul de transfer al fişierelor* (FTP) este dezactivat şi vă recomandăm să-l lăsaţi aşa;
- dezactivaţi opţiunea *Internet Service Manager* (HTML) pentru că un personaj negativ cu puţin mai multă experienţă într-ale dedesubturilor IIS-ului vă poate schimba paginile de pe serverul d-voastră de Web;
- dezactivaţi şi opţiunea de *SMTP Service* şi treceţi mai departe prin acţionarea butonului **OK**.

> *Notă*: Dacă se întrerupe curentul în timpul instalării sau configurării, nu intraţi în panică: luaţi-o cu calm de la capăt (pentru că toate setările şi personalizările efectuate în etapa aceasta au fost pierdute!) şi notaţi în planul d-voastră de achiziţii necesitatea unei surse neîntreruptibile de curent (UPS).

Serverul pe care îl instalăm în această etapă va fi configurat drept server de domeniu, de aceea noi dezactivăm opţiunea IIS.

Din componenta *Management and Monitoring Tools* vom activa *Network Monitor Tools* pentru că va fi nevoie de ea la urmărirea traficului pe reţea.

Celelalte componente pot rămîne neselectate în această etapă, dar dacă doriți să vă accesați serverul de pe altă stație sau dintr-o altă rețea, trebuie să activați opțiunea *Terminal Services*.

În total, după specificațiile de mai sus, componentele vor ocupa 30.2 Mb pe disc.

Treceți mai departe apăsînd butonul Next!

Pasul 11 – Personalizarea datei și a orei

De obicei data și ora sînt preluate automat din BIOS-ul sistemului, dar dacă există erori corectați-le. *Zona orară* (Time Zone) pentru România este GMT+2.

Pasul 12 – Parametrii de configurare a serviciului Terminal Services

Terminal Services este un serviciu care poate fi utilizat în două moduri:

- *în mod administrativ* (*remote administration mode*), posibilitate prin care un număr limitat de utilizatori se pot conecta la server de la distanță în scopuri administrative (numărul maxim de conexiuni este 2);
- *în mod server de aplicații* (*Application server mode*) – permite utilizatorilor care se conectează la server să ruleze una sau mai multe aplicații instalate pe acesta. Această modalitate este foarte uzuală în cazul rețelelor de calculatoare care utilizează sisteme de calcul perisate moral. Modul de licențiere este separat, fiecare stație client trebuind să aibă o licență de lucru individuală.

Pentru că serverul pe care-l instalăm nu va fi unul de aplicații, selectăm prima opțiune și trecem la pasul următor.

Pasul 13 – Setările pentru rețea

Această etapă începe cu instalarea componentelor, care durează aproximativ un minut (în funcție de configurația hardware pe care o aveți), după care trebuie să configurăm parametrii prin selectarea opțiunii *Custom Settings*. Din fereastra care urmează ne interesează opțiunea *Internet Protocol (TCP/IP)*. Click pe opțiunea specificată și apoi pe butonul **Properties**. În fereastra *Internet Protocol (TCP/IP) Properties* selectați opțiunea *Use the following IP address* și introduceți datele de identificare a serverului d-voastră în rețea.

> *Notă*: De unde știm care sînt datele de configurare pe care să le introducem în această etapă!? Într-unul din capitolele anterioare ați învățat cum se calculează adresele de rețea. În cazul în care serverul pe care îl folosiți se află într-o rețea nouă, atribuiți primul IP din plaja de IP-uri pe care ați obținut-o în urma calculelor. De exemplu, dacă doriți să realizați o rețea cu maximum 254 de host-uri, o adresă de rețea poate fi 172.172.172.0 cu valoarea 255.255.255.0 pentru Subnet Mask. Adresa pe care o vom folosi pentru primul server din rețea va fi 172.172.172.1. Nu este obligatoriu acest lucru!

În această etapă, cînd nu sînt cunoscute prea multe detalii, puteți completa doar cîmpurile *IP address* și *Subnet Mask*.

Puteți trece, apoi, mai departe la stabilirea apartenenței serverului la un domeniu de calculatoare (dacă există un astfel de domeniu configurat) sau într-un workgroup (grup de lucru) a cărui nume trebuie specificat în căsuța de text *Workgroup or computer domain*.

După specificarea numelui grupului de lucru (în cazul nostru *Grup1*) aplicaţia *Setup* transmite informaţiile de configurare în reţea pentru a verifica dacă nu există alte dispozitive în reţea care au acelaşi nume sau acelaşi IP.

Etapa ulterioară este aceea a copierii, instalării şi configurării componentelor specificate în etapele anterioare.

Ultima etapă, înaintea repornirii finale, este *Performing Final Tasks* în care se instalează căile scurte (shortcut) pentru anumite componente şi aplicaţii în meniul *Start*, se înregistrează componentele, se salvează setările şi se şterg fişierele temporare utilizate la procesul de instalare. Ultima intervenţie : la sfîrşit apăsaţi butonul **Finish**, repornirea calculatorului realizîndu-se automat.

Este posibil ca, în funcţie de dispozitivele hardware, după prima logare să vă apară un mesaj de repornire a calculatorului pentru iniţializarea corectă a acestora. În cazul în care unul dintre dispozitivele hardware nu se află în HCL (*Hardware Compatible List* – Lista dispozitivelor fizice compatibile), folosiţi driverele de instalare obţinute o dată cu achiziţia sistemului respectiv.

13.3. Configurarea serverului W2K în vederea realizării unui domeniu W2K

După prima conectare pe server se va deschide automat o fereastră de configurare (fig. 13.3.1) care vă poate ajuta să vă configuraţi serverul d-voastră, principalele opţiuni pe care le aveţi sînt :

- *Active directory* – serviciul pentru configurarea şi administrarea utilizatorilor dintr-un domeniu de calculatoare ;
- *File server* – server pentru fişiere ;
- *Print server* – server dedicat gestionării imprimantelor din reţea şi a accesului către acestea ;
- *Web/Media Server* – server dedicat publicării fişierelor HTML sau media pe Internet sau Intranet.

Scopul acestei etape din prezentul material este de a configura şi personaliza un server pentru un domeniu W2K de calculatoare.

Înainte de configurarea serviciului *Active Directory*, trebuie să ne îndreptăm puţin atenţia asupra discurilor şi a mediului W2K Server.

Principalele instrumente de administrare şi configurare se află în *Administrative Tools*, calea de a ajunge la ele este : **Start → Programs → Administrative Tools**.

Dacă nu le găsiţi aici încercaţi : **Start → Settings → Control Panel → Administrative Tools**.

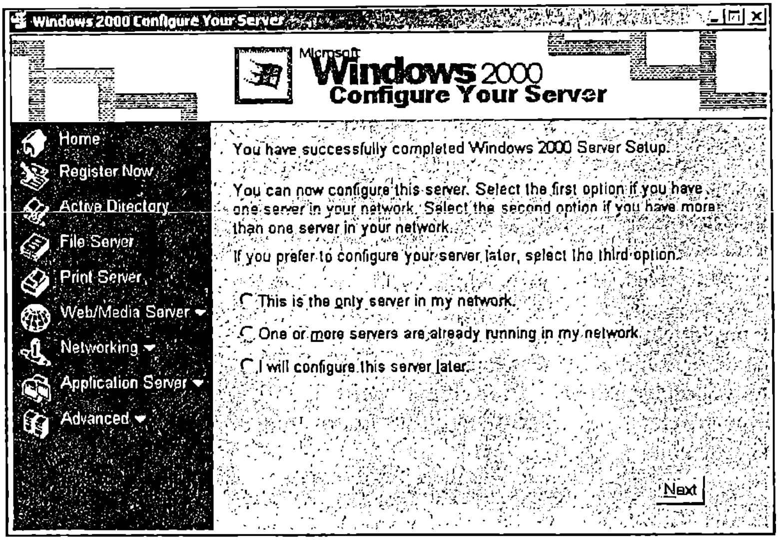


Figura 13.3.1. Fereastra de configurare a rolului serverului

Tabelul 13.3.1. Principalele instrumente de administrare

Categorie	Explicaţii
Component Services	Componenta de configurare şi gestionarea a aplicaţiilor COM+.
Computer Management	Conţine diferite instrumente pentru administrarea sistemului local, dar şi a altor sisteme precum şi gestionarea discurilor locale.
Configure Your Server	Personalizarea şi configurarea serviciilor Windows precum şi a componentelor de reţea. Aceasta este componenta care lansează aplicaţia prezentată în figura nr. 13.3.1.
Data Sources (ODBC)	Adăugarea, ştergerea şi configurarea componentelor ODBC (Open DataBase Connectivity).
Distributed File System	Componenta de creare şi gestionare a unui sistem de fişiere logic, compus din directoare puse la dispoziţie pe diferite calculatoare din reţea.

Categorie	Explicaţii
Event Viewer	Afişează diferite mesaje de la sistemul de operare precum şi de la alte aplicaţii.
Licensing	Gestionarea accesului clienţilor către diferite produse de tip server.
Local Security Policy	Vizualizarea şi modificarea politicilor locale de securitate, de exemplu, drepturile utilizatorilor.
Network Monitor	Capturarea pachetelor din reţea pentru a vă ajuta să detectaţi şi analizaţi diferite probleme din reţea.
Performance	Afişarea în mod grafic a performanţelor sistemului precum şi configurarea sistemului de înregistrare şi alertare.
Routing and Remote ...	Configurarea şi gestionarea serviciului de rutare precum şi a serviciului de acces la distanţă.
Services	Pornirea, configurarea şi oprirea serviciilor Windows.
Telnet Server Administration	Vizualizarea şi modificarea setărilor şi conexiunilor prin serviciul Telnet.
Terminal Services Cli...	Crearea suportului pentru instalarea clientului de conexiune la serverele de Terminal Services.
Terminal Services C...	Gestionarea parametrilor pentru Terminal Services.
Terminal Servic...	Gestiunea şi monitorizarea utilizatorilor de Terminal Services conectaţi la unul dintre serverele din reţea.

Pe lîngă anumite componente care au fost deja succint prezentate anterior, Computer Management include şi alte utilitare care vor fi prezentate în secțiunea următoare:

A. Event Viewer (aplicația de vizualizare a mesajelor despre diferite evenimente) include 3 categorii de înregistrări:

- monitorizarea mesajelor de la aplicațiile instalate;
- monitoarizarea mesajelor de securitate;
- monitorizarea mesajelor de sistem.

Pentru a vizualiza un mesaj în mod detaliat trebuie deschis prin dublu click. Există trei tipuri de mesaje: *Information* (mesaje de informare), *Warning* (mesaje de alarmă) şi *Error* (mesaje de eroare).

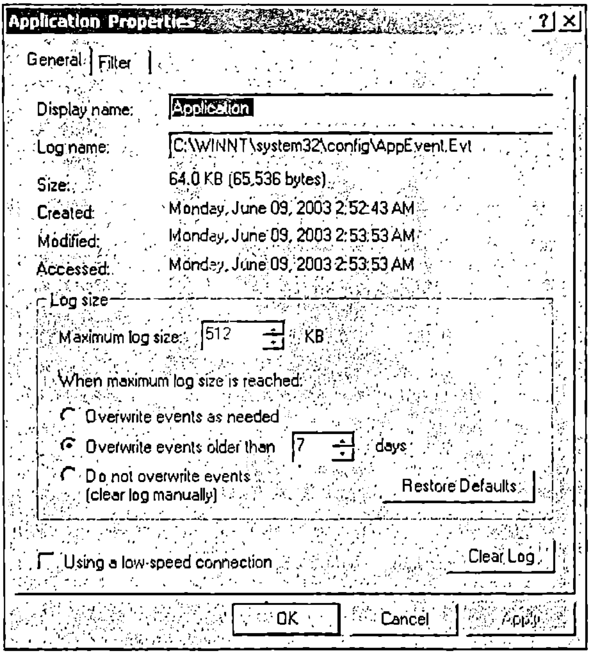


Figura 13.3.2. Fereastra de proprietăți a unei categorii de mesaje Application

Fiecare categorie din *Event Viewer* poate fi parametrizată, prin click dreapta al mouse-ului pe ea şi alegerea opțiunii **Properties** din meniul contextual afişat.

Principalele opțiuni sînt:

- *Maximum log size* (mărimea maximă a fişierului care stochează înregistrările) - exprimat în Kb. Vă recomandăm să măriți de 2-3 ori capacitatea de stocare a fişierului respectiv pentru fiecare categorie în parte.
- Acțiunea care se va efectua în momentul în care fişierul de log a ajuns la dimensiunea maximă unde putem alege: suprascrierea evenimentelor dacă este

nevoie (*Overwrite events as needed*); suprascrierea evenimentelor mai vechi de 7 zile; ştergerea manuală a înregistrărilor.

- Ştergerea cu posibilitatea de salvare a înregistrărilor (butonul *Clear Log*). Înregistrările din Event Viewer pot fi salvate în formatul proprietar *EVT* sau într-un format mai larg *CSV* (*coma separated value*) care permite importul şi analiza informaţiilor în aplicaţii de calcul tabelar şi nu numai.

Nu mai insistăm prea mult pe acest utilitar, pentru că vom reveni într-un capitol separat de monitorizare şi înregistrare a accesului. Trebuie, în schimb, să menţionăm că, pînă în momentul în care nu se activează politica de securitate pe sistemul local sau pe domeniu, în categoria *Security* nu se va înregistra nici un mesaj.

Nu recomandăm activarea politicii de securitate în această etapă, dar pentru a realiza totuşi această operaţiune trebuie să parcurgeţi următoarele etape:

1. **Start → Programs → Administrative Tools → Local Security Policy**.
2. În fereastra *Local Security Settings* în categoria *Local Policies* activaţi de la subcategoria *Audit Policy* opţiunile pentru: *Audit account logon events*, *Audit account management*, *Audit logon events*, *Audit policy change*.
3. După efectuarea schimbărilor respective şi închiderea ferestrelor deschise, redeschizînd Event Viewer o să constataţi că deja au început să apară înregistrări în *Security*.

B. System information – oferă un set de informaţii generale asupra sistemului curent grupate pe 5 categorii, neconfigurabile.

C. Shared Folders – prezintă informaţii despre:

- *directoarele puse la dispoziţie în reţea* (*Shares*) cu posibilitatea schimbării permisiunilor sau a datelor despre share-ul respectiv precum şi a creării de noi informaţii shared. Informaţiile shared implicite sînt: *discurile locale* (în cazul nostru, singurul disc existent este C$), directorul *WinNT* care poartă numele de share *Admin$*, precum şi share-ul *IPC$* care este destinat utilizatorilor din reţea în vederea conectării la viitoarele imprimante, instalate în sistem. Comanda pentru punerea la dispoziţie a unei informaţii în reţea este *net share*. Un mod de apelare şi utilizare a unei resurse puse la dispoziţie în reţea se poate realiza cu ajutorul comenzii *net use*.

> *Notă*: Toate share-urile care sînt postfixate cu caracterul dolar ($) sînt cunoscute sub denumirea de share-uri administrative. Administratorul unui sistem poate crea share-uri administrative sub rezerva faptului că acestea nu sînt vizibile în mod normal în reţea. Acest mod de creare a share-urilor este recomandat pentru ascunderea informaţiilor private.

- *sesiunile deschise pe sistemul curent* (*Sessions*) cu posibilitatea deconectării unui utilizator sau a închiderii unei sesiuni. Această opţiune este echivalenta comenzii *net sessions*.
- *fişierele deschise de pe sistemul curent* (*Open Files*) – în care se specifică numele utilizatorului, numele fişierului deschis, calea de pe server în care se află fişierul respectiv precum şi modul de deschidere a fişierului: pentru citire (*read*), scriere

și citire (*Write* + *Read*). Comanda folosită în mod text pentru vizualizarea acestor informații este *net file*.

D. Device manager - folosit pentru afișarea informațiilor și configurarea dispozitivelor hardware.

E. Local Users and Groups este opțiunea care nu apare pe serverele configurate ca servere de domeniu și care permite crearea de utilizatori și grupuri de utilizatori locali.

Crearea unui utilizator local:

1. În Local User and Groups, RClick **Users → New User**.
2. Scrieți numele de utilizator la căsuța *User Name*, numele complet la *Full Name*, o scurtă descriere la *Description*, parola și confirmarea parolei la *Password* și *Confirm password*.
3. **Create**.

Cele 4 opțiuni din fereastra de creare a utilizatorilor vor fi detaliate în capitolul dedicat Active Directory.

F. Configurarea discurilor (*Disk Management*)

Una din cele mai importante opțiuni este configurarea discurilor, opțiune care poate fi accesată din **Computer Management → Storage → Disk Management**.

Dacă serverul d-voastră este dotat cu mai multe hard discuri SCSI, se va declanșa automat aplicația de semnare a discurilor (*Write Signature and Update Disk Wizard*) care vă va ajuta să vă configurați un sistem de organizare RAID (*Redundant Array of Independent Disks*) a discurilor d-voastră.

Parcurgeți pas cu pas etapele semnării discurilor, nu înainte de a le selecta din lista care apare după fereastra de întîmpinare. După terminarea acestei etape, toate discurile în afară de discul 0 (primul disc) sînt dinamice, adică pot fi configurate în partiții RAID.

Pentru a include și primul disc într-un sistem RAID, trebuie transformat și acesta într-un disc de tip dinamic:

1. RClick pe **primul disc → Upgrade to Dynamic Disk → OK**.
2. **Upgrade** în fereastra *Disks to Upgrade* → **Yes** în fereastra de informare *Disk Management*.
3. Click **Yes** în fereastra de atenționare *Upgrade Disks*, click **OK** în fereastra de confirmare a acțiunii de repornire a serverului.
4. După repornire, trebuie să mai efectuați încă o dată operațiunea de repornire, pentru inițializarea corectă a discurilor. Se poate continua și fără această nouă operațiune de repornire, dar nu vă recomandăm pentru că este posibil să obțineți anumite erori în procesul de configurare dinamică a discurilor.

Notă: Dacă aveți un singur disc, nu sînt necesare aceste operațiuni.

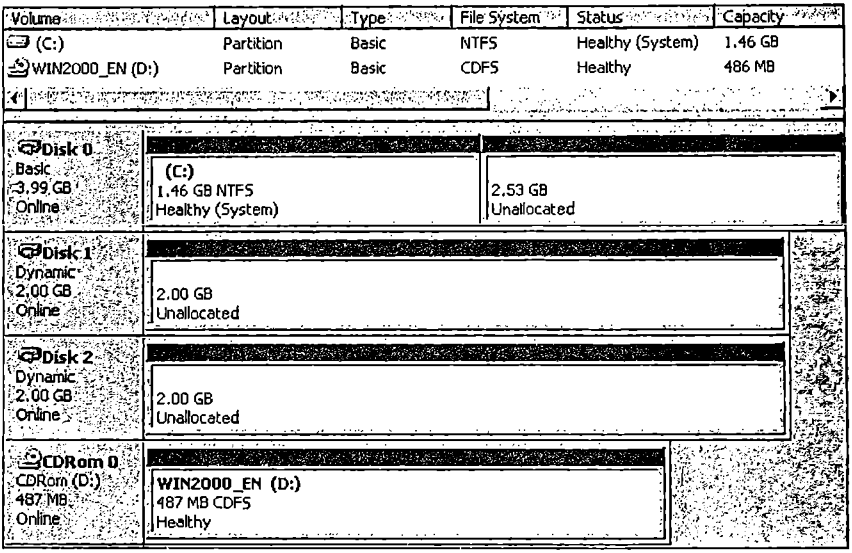


Figura 13.3.3. Fereastra de prezentare a 3 discuri neconfigurate în Disk Management

După repornire, intraţi din nou în Computer Management la Disk Management şi veţi observa în acest moment că şi discul 0 este dinamic. Acest lucru vă permite o clonare a partiţiei de startare a sistemului de operare pe oricare dintre discurile 1 sau 2:

1. RClick pe partiţia C: → **Add Mirror**.
2. Alegeţi din fereastra în care apare Discul 1 → **OK** → **OK** în fereastra de atenţionare cu privire la schimbările pe care trebuie să le efectuaţi în fişierul *boot.ini* pentru a putea porni sistemul de operare de pe al doilea disc. Această operaţiune este foarte utilă pentru siguranţa sistemului d-voastră, pentru că, dacă unul din discurile 0 sau 1 suferă o defecţiune fizică, veţi putea folosi serverul fără nici o problemă, sistemul de operare fiind salvat şi pe al doilea disc (Disk 1).
3. Urmează un proces de regenerare a fişierelor sistemului de operare (*Regenerating*).

Spaţiul rămas liber după operaţiunea de protejare în oglindă poate fi transformat în partiţii:

1. RClik (pe spaţiul nealocat) → **Create Volume** → Next.
2. Pe sistemele pe care sînt instalate mai multe discuri putem crea următoarele tipuri de partiţii:
   - *Simple volume* – utilizează spaţiul de pe un singur disk. În fereastra care urmează după apăsarea butonului Next, avem posibilitatea de specificare a dimensiunii noii partiţii, dimensiune care nu poate depăşi spaţiul maxim disponibil. La pasul următor, se asignează o literă noii partiţii, apoi la următoarea fereastră (fig. 13.3.4) se specifică sistemul de fişiere care va fi utilizat (*File System to use*): FAT, FAT32, recomandarea noastră fiind NTFS, la *Volume label* specificaţi o etichetă dorită pentru partiţia respectivă (de exemplu,

Users), iar pentru a economisi timp, activați opțiunea *Perform a Quick Format*. După ce apăsați **Next**, în ultima fereastră apăsați butonul **Finish**.

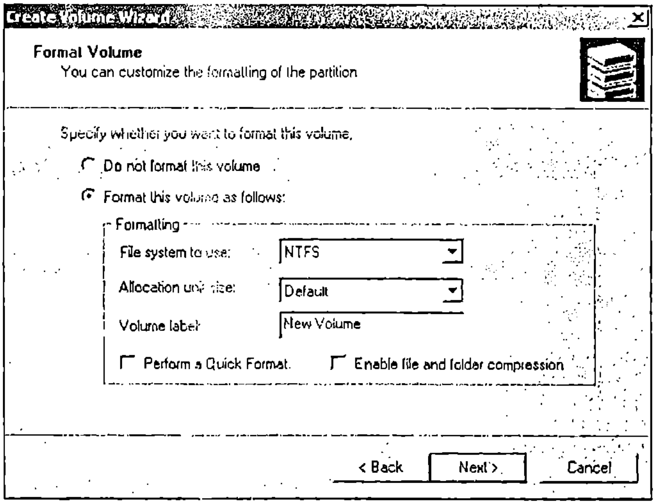


Figura 13.3.4. Fereastra de formatare a partițiilor

- o *Spanned volume* – presupune crearea unei partiții prin alocarea de spațiu de pe mai multe discuri, sau de pe toate discurile. Se poate crea o partiție din tot spațiul rămas pe discuri sau numai de pe o parte din discuri, sau numai o parte din spațiul disponibil. Suma alocărilor de pe fiecare disc reprezintă volumul total al viitoarei partiții.
- o *Striped volume* – presupune crearea unei partiții utilizînd spațiul de pe 2 sau mai multe discuri, prin alocarea aceluiași spațiu pe fiecare din discurile alese, volumul total al viitoarei partiții fiind egal cu nr.discurilor*spațiul alocat.

Notă: Ștergerea unei partiții: RClick (pe partiția care se dorește a fi ștearsă, în afară de partiția system) → Delete volume → Yes

- o *RAID-5 volume* – presupune alocarea de spațiu egal de pe fiecare disc, dimensiunea totală a viitoarei partiții fiind egală cu nr.partițiilor*volumul_alocat – volumul_alocat pe o partiție. Avantajul acestor tipuri de partiții este acela că securitatea datelor este mult mai bună decît în cazul celorlalte tipuri, alt avantaj fiind viteza de acces la date mai mare.

În cazul în care aveți prea multe partiții și acest lucru vă provoacă probleme privind gestionarea acestora, vă recomandăm schimbarea literelor partițiilor, precum și a etichetelor acestora, corespunzător destinației fiecărei partiții.

În figura nr. 13.3.5 este prezentată o posibilă structură pentru un server de domeniu:

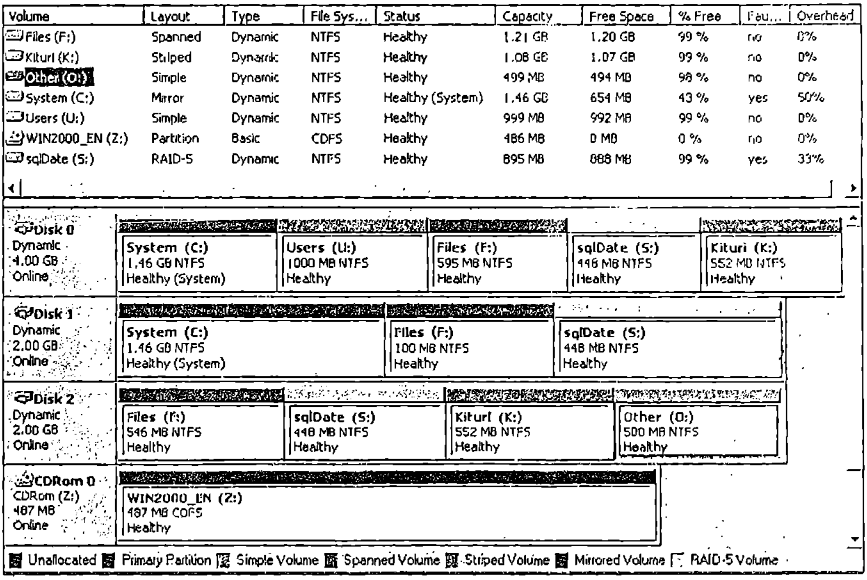


Figura 13.3.5. Configuraţia discurilor

Schimbarea etichetei unei partiţii: RClick pe partiţie → **Properties** → introduceţi noua etichetă în căsuţa *Label* → **OK**.

Schimbarea literei unei partiţii: RClick pe partiţie → **Change Driver Letter and Path** → **Edit** → alegeţi o literă disponibilă din lista *Assign a drive letter* → **OK** → **Yes** în fereastra *Confirm*.

13.4. Crearea unui server pentru un nou domeniu

Una dintre cele mai importante etape în realizarea unei reţele Windows este aceea de creare a unui nou domeniu.

În Windows NT 4.0, serverele de domenii puteau fi de 2 tipuri: *Primary Domain Controller* (PDC) şi *Backup Domain Controller* (BDC), într-o reţea neputînd exista decît un singur PDC şi de la unul la mai multe BDC-uri. Configurarea ca PDC sau BDC se realiza de la instalare.

În Windows 2000, serverul este un termen generic, care poate fi configurat în funcţie de necesităţi. Un server de domeniu este recunoscut generic sub denumirea de *Domain Controler* (DC), într-o reţea putînd exista mai multe astfel de servere care partajează informaţia din Active Directory în scopul unei mai mari siguranţe a reţelei.

Proprietatea de Domain Controler este văzută în Windows 2000 ca un *rol* care poate fi schimbat uşor între diferitele servere din reţea, asigurînd astfel o mai mare flexibilitate a reţelei. În unele cazuri, primul server care a fost configurat ca DC în reţea este recunoscut şi ca *Master Domain Controller* (MDC), toate celelalte servere fiind *Secondary Domain Controller* (SDC).

Instalare Active Directory

Pasul 1 - Lansarea în execuție a ferestrei de configurare

Start → Programs → Administrative Tools → Configure Your Server.

Pasul 2 - Instalare Active Directory

În fereastra care s-a deschis se apasă pe *Active Directory* și în josul ferestrei există hyperlink-ul *Start*.

În fereastra de *Welcome* apăsați Next, apoi în alegerea tipului serverului : pentru un domeniu nou (*Domain controller for a new domain*) sau ca un server suplimentar pentru un domeniu existent (*Additional domain controller for an existing domain*).

Atenție : Dacă aveți conturi de utilizatori locale precum și alte setări de securitate și căsuțe de e-mail pe serverul pe care doriți să configurați Active Directory, aceste vor fi șterse automat.

În cazul nostru, instalînd primul server, vom alege prima opțiune și trecem la etapa următoare.

Pasul 3 - Crearea unui arbore de domenii

În Active Directory rețelele locale sînt organizate arborescent, momentul configurării primului server din rețea coincide cu crearea unui nou arbore de domenii. Alegeți, așadar, prima opțiune (*Create a new domain tree*) și treceți la pasul următor unde va trebui să creați o nouă „pădure" (*forest*).

Pasul 4 - Crearea unui nou nume de domenii

Active Directory presupune existența unei alte structuri arborescente care reprezintă scheletul de comunicație între stațiile din viitorul domeniu. Acest nou serviciu care trebuie instalat este DNS (*Domain Name System* - Sistemul numelor de domenii).

Programele utilizate, în mod curent, se referă rareori la sistemele gazdă, cutii poștale și alte resurse prin adresa lor binară (IP), în locul acesteia fiind folosite șiruri de caractere de forma :

nume_host.subdomeniu1...subdomeniu_n.domeniu

Folosirea unor șiruri de caractere în locul adreselor binare duce la utilizarea ușoară a adreselor, fiind mult mai ușor de reținut decît niște numere care nu spun mare lucru utilizatorilor obișnuiți. Va fi necesar un mecanism care să permită convertirea unei adrese din format ASCII în format IP, singurul format recunoscut în rețea. De exemplu, rețeaua ARPANET avea un site ce conținea un fișier text numit host.txt, care cuprindea toate sistemele gazdă și adresele lor. Conversia între adrese era realizată pe baza acestui fișier, însă această modalitate este rezonabilă doar într-o rețea ce conține cîteva sute de mașini gazdă.

Structura arborescentă a DNS permite utilizarea de domenii cu același nume. Pentru a se stabili corespondența între nume și adresa IP se procedează astfel :

- programul de aplicație apelează o procedură de bibliotecă (*resolver*), transferîndu-i ca parametru numele de domeniu ;
- resolver-ul trimite un pachet UDP la serverul local DNS, care caută numele și returnează adresa IP asociată acestuia ;
- avînd adresa IP, programul apelant poate stabili o conexiune TCP cu destinația.

Extinderea domeniilor de la diferite niveluri ale arborelui DNS se poate realiza prin crearea de proxy servere, care permit calculatoarelor unei reţele să acceseze în sens unic resursele reţelei Internet, acestea nefiind „văzute" din exterior.

În Windows 2000 Server, numele de DNS conţine şi numele de *NetBIOS* al viitorului nume al domeniului de calculatoare.

În cazul nostru, vom folosi drept denumire a domeniului *mydom.myorg.ro*. Numele complet al fiecărei staţii din viitorul domeniu va fi format din numele acesteia (*NetBIOS Name*) urmat de numele domeniului DNS.

Pasul următor este reprezentat de specificarea numelui de NetBIOS al domeniului, propunerea implicită fiind reprezentată de prima categorie : *mydom*.

Locaţia implicită a bazei de date cu informaţiile din Active Directory este în directorul WINNT, subdirectorul NTDS, pe discul pe care a fost instalat sistemul de operare (în cazul nostru, partiţia C :). Această locaţie poate fi schimbată (prin apăsarea butonului *Browse*), dar nu vă deranjează cu nimic dacă rămîne acolo. De asemenea, log-urile (jurnalul de activitate) sînt salvate implicit la aceeaşi adresă de pe disc.

Pentru ca anumite obiecte din Active Directory să poată fi accesibile din orice punct al reţelei, acestea trebuie să fie puse la dispoziţie în reţea prin crearea unui share. Locul de salvare a acestor obiecte este în directorul WINNT, subdirectorul SYSVOL. Vă recomandăm să folosiţi opţiunile implicite !

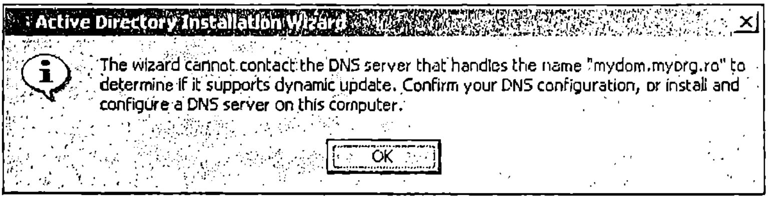


Figura 13.4.1. Fereastra care precedă instalarea serviciului DNS

Apariţia ferestrei de informare din figura 13.4.1 denotă faptul că în reţeaua d-voastră nu există nici un server configurat ca DNS care să poarte numele specificat într-o etapă anterioară. Utilitarul de instalare şi configurare a Active Directory vă oferă posibilitatea de configurare în această etapă a acestui serviciu.

Apăsaţi butonul **OK** şi alegeţi opţiunea de instalare şi configurare automată (recomandată) a serviciului DNS pe calculatorul curent.

Pasul 5 – Permisiunile

Această etapă este foarte importantă din punctul de vedere al structurii reţelei d-voastră. Prima opţiune (*Permissions compatible with pre-Windows 2000 servers*) vă oferă posibilitatea de a conecta la serverul d-voastră staţii care au instalat sisteme de operare mai vechi decît Windows 2000. A doua opţiune (*Permissions compatible only with Windows 2000 servers*) asigură o securitate mult mai bună domeniului d-voastră.

În cazul în care toate staţiile şi serverele din domeniul d-voastră au drept sistem de operare Windows 2000 sau un sistem Windows mai nou, vă recomandăm cu căldură a doua opţiune. Dacă nu, atunci obligatoriu este să folosiţi prima opţiune.

În cazul în care pe viitor pot exista căderi ale serviciului Active Directory, serverul poate fi pornit în *Directory Service Restore Mode* care permite o recuperare a informațiilor. Pentru accesul la această opțiune aveți nevoie de o parola pe care o puteți specifica în fereastra următoare. Pentru a accesa opțiunea de *Restore*, introduceți CD-ul cu kit-ul de instalare a sistemului de operare în unitatea de CD-ROM și reporniți sistemul. După repornire, se lansează aplicația *Setup* de pe CD și alegeți opțiunea *Restore* (tasta **R**).

Pasul 6 - Ultima etapă

Ultima etapă ne prezintă un scurt sumar al informațiilor configurate, după care se trece la configurarea efectivă a Active Directory.

Pentru a putea configura Active Directory aveți nevoie de CD-ul de instalare a sistemului de operare W2K Server. Într-o etapă anterioară, litera CD-ROM-ului a fost schimbată cu **Z**: așa că fișierele de instalare trebuie căutate la această nouă locație, în directorul *I386* de pe discul d-voastră.

Finalizarea instalării presupune în același timp repornirea serverului pentru inițializarea noilor parametri de configurare a acestuia.

După repornire, în fereastra de conectare (*Log On to Windows*) apare o nouă listă de opțiuni din care puteți alege domeniul la care vă veți conecta. Pe fiecare stație de lucru inclusă în viitorul domeniu va apărea, pe lîngă numele domeniului, numele de NetBIOS al stației.

Pentru a nu mai vizualiza de fiecare dată la repornire fereastra de configurare a serverului, dezactivați opțiunea *Show this screen at startup* și închideți fereastra.

Una dintre ultimele modificări pe care trebuie să le efectuați este reprezentată de schimbarea adresei DNS de la configurarea adaptorului de rețea din 127.0.0.1 (adresa de loopback) în adresa serverului care reprezintă în acest moment și server de DNS:

1. RClick (pe pictograma *My Network Places*) → **Properties**.
2. RClick (pe *Local Area Connection*) → **Properties**.
3. **Internet Protocol (TCP/IP)** → **Properties** → introduceți adresa serverului la secțiunea *Prefered DNS server* → OK → (pentru vizualizarea în bara de aplicații a informațiilor despre conexiunea la rețea, activați opțiunea *Show icon in taskbar when connected*) → **OK**.

Dezinstalarea serviciului Active Directory

Această opțiune permite administratorilor de sistem schimbarea destinației unui server din cadrul unei rețele. Alte cazuri în care această opțiune se poate aplica este aceea în care unui server i se atribuie rolul de server de Web într-un domeniu.

Pentru acest lucru trebuie să parcurgeți următoarele etape:

1. **Start** → **Run** → scrieți *dcpromo* → **OK** → **Next**.
2. În fereastra de informare (fig. 13.4.2) apăsați OK.
3. În cazul în care nu aveți un server de domeniu secundar, toate informațiile despre conturile de utilizatori vor fi eliminate, de asemenea politicile de securitate precum și cheile publice de acces la diferite resurse. Domeniul nu va mai exista! Selectați opțiunea *This server is the last domain controller in the domain* în cazul în care nu mai există nici un alt server de domeniu în rețea și apăsați **Next**.

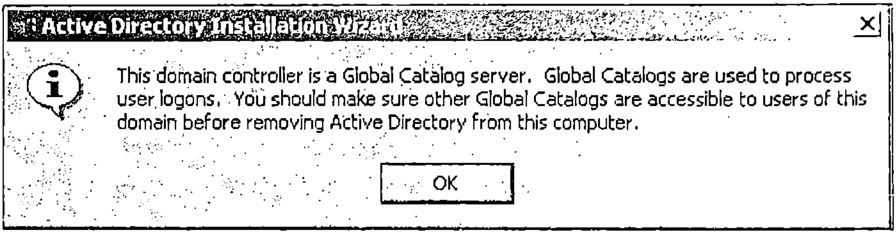


Figura 13.4.2. Fereastra de informare privind rolul serverului în reţea

4. Introduceţi parola administratorului de domeniu, urmată de confirmarea acesteia → **Next** → **Next** → **Finish**.
5. Reporniţi sistemul.

Desigur că dacă doriţi să creaţi un nou domeniu, puteţi parcurge paşii de la capitolul anterior.

13.5. Instalarea Windows XP în mod automat

Pe CD-ul d-voastră de instalare în calea \Support\Tools\Deploy.cab\ există mai multe fişiere executabile destinate pregătirii instalării automate a sistemului de operare WindowsXP, cel mai important fiind *setupmgr.exe*.

Copiaţi fişierele într-o anumită locaţie pe discul d-voastră şi lansaţi în execuţie.

Pasul 1 – Fereastra de întîmpinare

Citiţi dacă vă interesează şi apăsaţi Next.

Pasul 2 – Crearea unui nou fişier de răspuns

Fişierul *unattended* care se va crea reprezintă un fişier de răspunsuri destinat instalării, echivalentul click-urilor care se dau la instalarea clasică.

Din cele 2 opţiuni alegeţi prima opţiune : *Create a new answer file* după care apăsaţi butonul Next.

Pasul 3 – Stabilirea tipului de instalare

Există 3 modalităţi de instalare automată a sistemelor de operare Windows :

- Windows Unattended Installation (WUI) ;
- Sysprep Install (SyI) ;
- Remote Installation Services (RIS).

Vom detalia pe parcurs aceste moduri de instalare.

Alegeţi prima variantă (WUI) şi apăsaţi butonul **Next**.

Pasul 4 – Alegerea platformei care va fi instalată

- Windows XP Home Edition ;

- Windows XP Professional ;
- Windows 2002 Server, Advanced Server or Data Center.

În cazul nostru, alegem varianta a doua şi trecem la pasul următor.

Pasul 5 - Selectarea modului de interacţiune a instalării cu utilizatorul

Opţiunea a doua *Fully automated* este cea pe care o recomandăm pentru că ocupă cel mai puţin timp operatorilor de reţea.

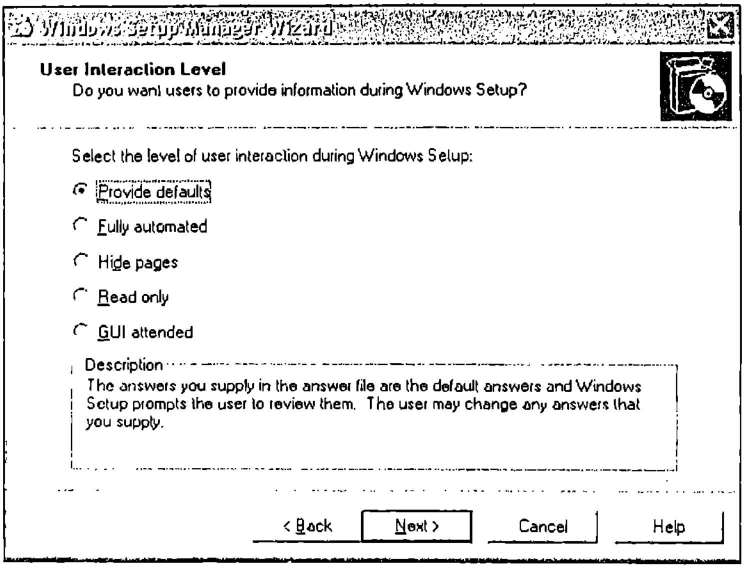


Figura 13.5.1. Modul de interacţiune cu utilizatorul în timpul instalării

Pasul 6 – Stabilirea locaţiei fişierelor de instalare

În momentul instalării, după cum v-aţi imaginat, este nevoie şi de fişiere, care pot fi postate undeva pe un director accesibil din reţea sau de pe CD-ROM-ul original. Avantajul creării unui director pe disc este acela al vitezei de accesare, mai ales dacă instalarea se realizează de pe un server cu discuri SCSI.

Alegeţi aşadar varianta 1 şi treceţi mai departe.

Pasul 7 - Specificarea locaţiei fişierelor de instalare

În mod uzual, instalarea se realizează de pe CD (prima opţiune), dar pot exista şi cazuri în care fişierele de instalare (kit-ul de instalare) se află pe un anumit disc local sau din reţea care vor fi localizate prin apăsarea butonului *Browse*.

În cazul nostru, fişierele de instalare sînt localizate pe CD-ROM. Activăm aşadar opţiunea *Copy the files from CD* şi trecem la pasul următor.

Excepţie:	În cazul în care veţi întîmpina mesajul de eroare prezentat în figura 13.5.2, apăsaţi butonul **OK**, şi din fereastra anterioară alegeţi a doua opţiune, apăsaţi butonul Browse şi localizaţi fişierul *dosnet.inf* din directorul I386 de pe CD-ROM, apăsaţi butonul **Open** şi după aceea treceţi în sfîrşit la pasul următor.

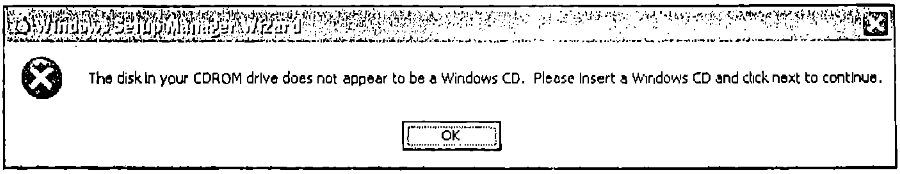


Figura 13.5.2. Mesaj de eroare

Pasul 8 – Stabilirea locaţiei şi a numelui directorului pentru distribuţia instalării

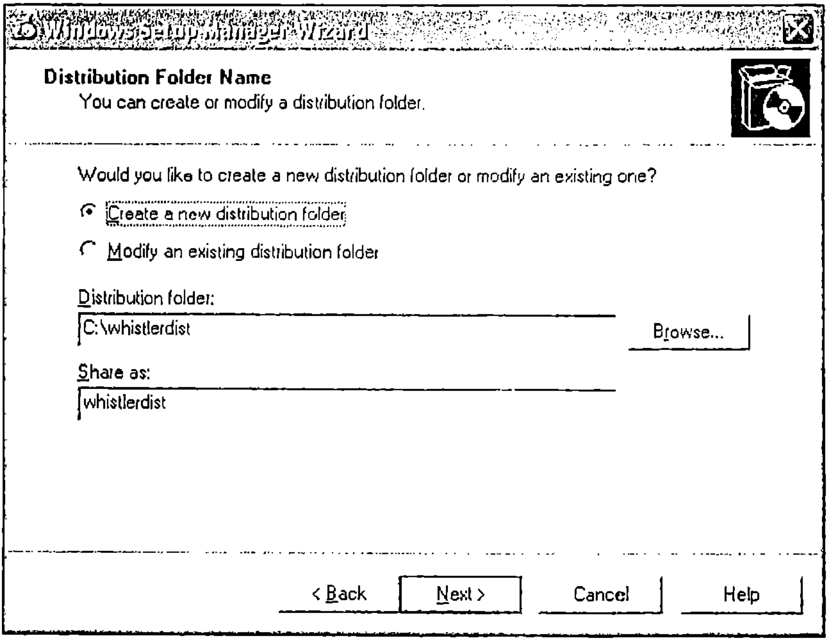


Figura 13.5.3. Stabilirea locaţiei punctului de distribuţie

Dacă sînteţi la prima instalare, veţi folosi opţiunea *Create a new distribution folder*. Acest nou director poate fi creat pe discul C: sau pe oricare disc pe care îl puteţi schimba apăsînd pe butonul **Browse**. Pentru a putea fi accesat prin reţea, directorul trebuie să poarte un sharename, implicit fiind whistlerdist. De asemenea, şi acest sharename poate fi schimbat, noi o să exemplificăm pe valorile implicite (nu vom schimba aceste valori) şi trecem la pasul următor.

Pasul 9 – Acceptarea licenței

Pentru a putea instala un sistem de operare sau oricare altă aplicație, trebuie să acceptăm condițiile și termenii de utilizare a acestora. Activați, așadar, opțiunea *I Accept the terms of the License Agreement* și treceți la pasul următor.

Pasul 10 – Personalizarea instalării

Fereastra *Windows Setup Manager Wizard* se închide automat și putem personaliza în continuare instalarea automată, în această secțiune stabilindu-se parametrii echivalenți etapei GUI din instalarea clasică.

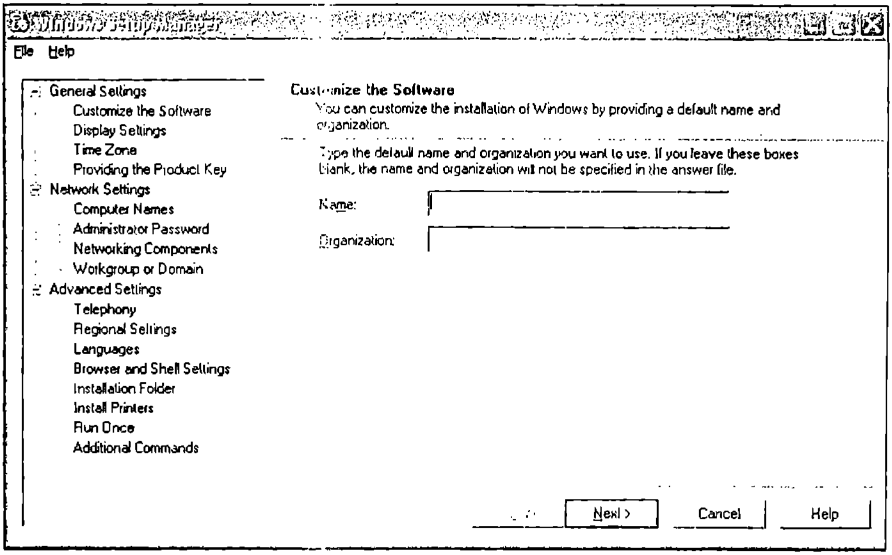


Figura 13.5.4. Fereastra de personalizare a instalării

În această parte se specifică un anumit nume de utilizator (*Name*) (de obicei, numele celui căruia îi aparține licența) precum și numele organizației care a achiziționat respectiva licență de utilizare (*Organization*).

Pasul 11 – Stabilirea parametrilor pentru display

În această etapă se stabilește numărul de culori care vor fi folosite în viitor (adîncimea culorii): 16, 256, High Color (16 bit), True Color (24 bit), True Color (32 bit). Stabiliți numărul de culori în funcție de resursele hardware pe care le dețineți.

În lista *Screen area* se stabilește rezoluția pe care o veți utiliza în viitor, rezoluția comună fiind: 1024x768, dar puteți opta și pentru versiunile 640x480, 800x600, 1280x1024, iar la lista *Refresh frequency* se stabilește frecvența cu care vor lucra calculatoarele d-voastră. În acest exemplu vom utiliza o frecvență comună 75 Hertz.

În cazul în care una sau mai multe valori specificate în listele din această fereastră nu corespund valorilor pe care le doriți, puteți personaliza valorile respective apăsînd butonul **Custom** (fig. 13.5.5).

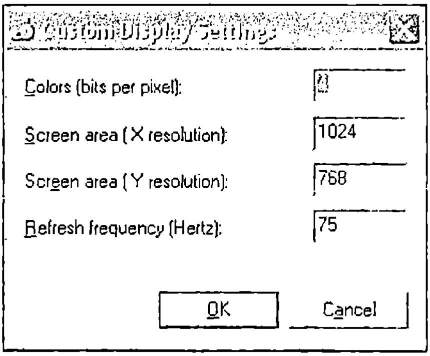


Figura 13.5.5. Personalizarea valorilor pentru Display

Pasul 12 – Time Zone

În această etapă se stabileşte tipul de oră corespondent locaţiei geografice a viitoarelor staţii de lucru. Pentru România, valoarea care se selectează din listă este: (GMT+02:00) Bucharest.

Pasul 13 – Introducerea cheii de instalare a produsului

În mod normal, această cheie, care verifică autenticitatea produsului, se află specificată în licenţa oferită de firma furnizoare a staţiei de lucru, pe CD-ul de instalare sau pe coperta acestuia.

Pasul 14 – Detalii despre staţiile care vor fi instalate

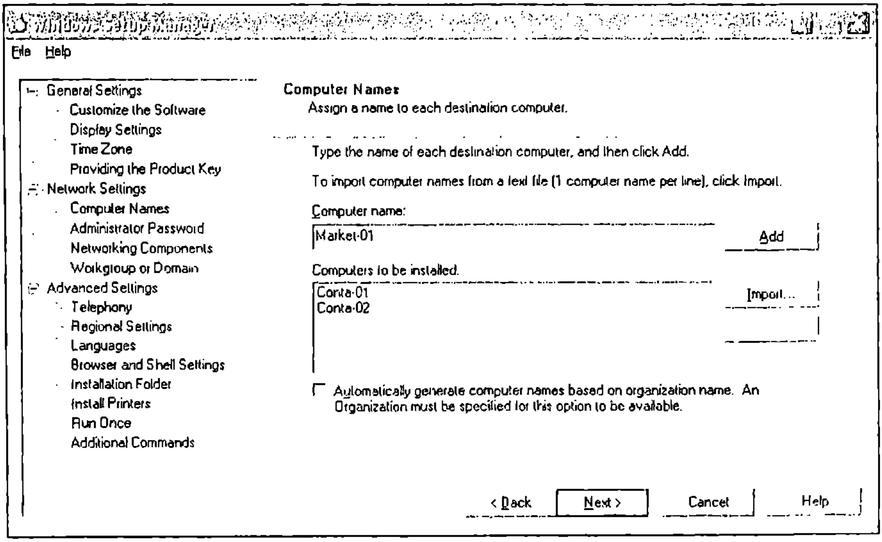


Figura 13.5.6. Declararea staţiilor care vor fi instalate în mod automat

În această etapă se specifică numele tuturor staţiilor din reţea care vor fi instalate în mod automat. Nu cunoaştem o limitare a numărului de staţii care pot fi specificate în acest moment. În urma acestei etape va fi creat un fişier care va conţine detalii despre fiecare staţie.

În cazul în care nu cunoaştem denumirea fiecărei viitoare staţii, putem activa opţiunea *Automatically generate computer name based on organization name*, care presupune generarea automată de denumiri de staţii de lucru.

Pasul 15 - Specificarea parolei pentru utilizatorul Administrator

Opţiunea este activată implicit cu scopul de a obliga pe cel care realizează instalarea să activeze această opţiune. Numărul maxim al caracterelor care pot fi specificate este de 127.

În cazul în care se doreşte o securizare a parolei pentru administratorul local, activaţi opţiunea *Encrypt administrator password in answer file* şi dacă se planifică alte instalări ulterioare, se poate activa opţiunea *When the computer starts, automatically log on as Administrator* cu posibilitatea de a alege numărul de log on-uri ulterioare. *Atenţie!* Această informaţie este trecută în regiştrii sistemului de operare aşa că nu specificaţi un număr prea mare la opţiunea *Number of times to auto log on*.

Pasul 16 - Personalizarea datelor de conectare în reţea

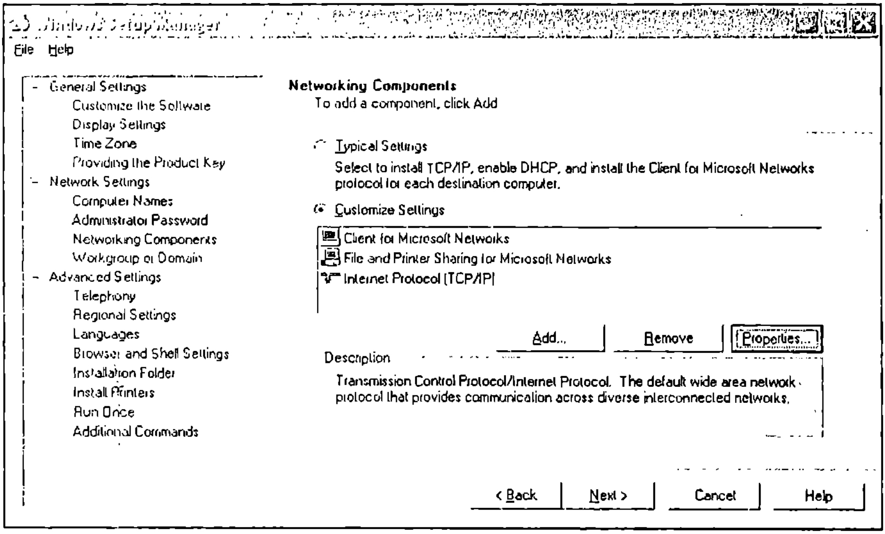


Figura 13.5.7. Configurarea adreselor IP

În mod implicit este activată opţiunea *Typical Settings*, care presupune existenţa unui server DHCP în reţea, care să permită alocarea dinamică de IP-uri.

În cazul în care doriţi ca fiecare staţie de lucru din viitoarea reţea să dispună de propriul IP, vă recomandăm să alegeţi opţiunea a doua: *Customize Settings* după care selectaţi opţiunea *Internet Protocol (TCP/IP)* şi apoi butonul **Properties** şi completaţi căsuţele *IP address*, *Subnet Mask*, *Default Gateway*, *Primary DNS server* şi eventual (opţional) *Secondary DNS server* cu valori specifice reţelei d-voastră de calculatoare.

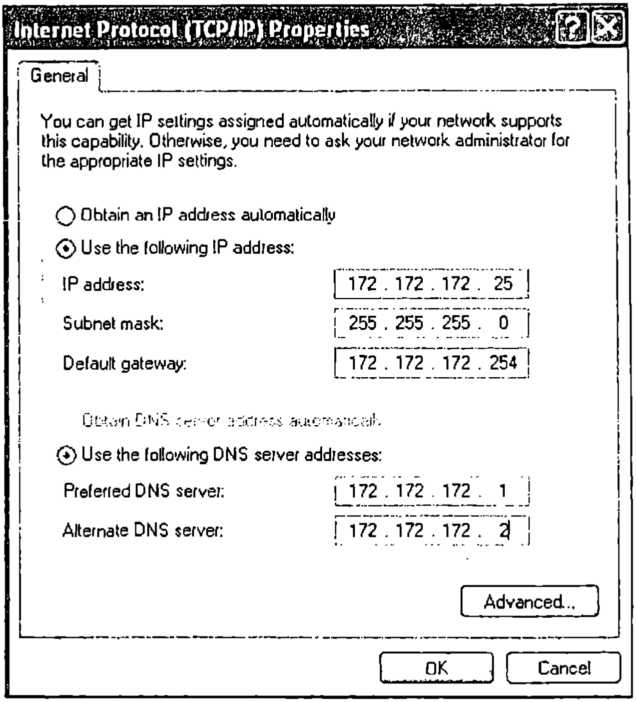


Figura 13.5.8. Proprietăţile protocolului TCP/IP

În cazul în care doriţi instalarea unor servicii de reţea suplimentare, activaţi butonul **Advanced**. În exemplul nostru mergem pe varianta implicită.

Pasul 17 - Specificarea apartenenţei la un Workgroup sau la un domeniu

O staţie/calculator poate aparţine unui grup de calculatoare (*workgroup*) sau, în cazul în care aţi configurat deja un domeniu, poate aparţine acestuia. În cazul nostru domeniul se numeşte *MYDOM*, utilizatorul care are dreptul de adăugare a unei noi staţii în domeniu este Administrator, iar parola este ***... ş.a. după care se trece la pasul următor.

Pasul 18 - Parametrii pentru telefon

Aceste informaţii se configurează numai pentru sistemele care deţin un modem şi care vor fi conectate la Internet prin intermediul acestuia. În cazul în care nu deţineţi un astfel de echipament treceţi la pasul următor.

Pasul 19 - Personalizarea regiunii

Poate fi configurată de cei care doresc să-şi personalizeze modul de afişarea a informaţiilor de sistem (dată, oră, simboluri monetare etc.) într-o altă limbă/formă decît în engleză.

Noi vom folosi în acest exemplu valorile implicite.

Pasul 20 - Adăugarea de opțiuni suplimentare pentru limbajul tastaturii

Se folosește pentru a adăuga noi limbaje pentru tastaturi. Spre exemplu, pentru a adăuga o tastatură românească trebuie selectată din listă opțiunea *Central Europe*.

Pasul 21 - Personalizarea Browserului de Internet

Se poate folosi opțiunea implicită *Use default Internet Explorer settings* sau, în cazul în care se dorește specificarea unei pagini de start (*home page*), se apasă butonul **Browser Settings** și la *Home page* se trece adresa paginii dorite. De asemenea, se pot adăuga adrese favorite.

Pasul 22 - Specificarea numelui directorului de instalare

Implicit, numele directorului în care se vor instala fișierele sistemului de operare Windows XP este *Windows*. Acest nume poate fi schimbat, dar nu recomandăm acest lucru pentru că anumite aplicații pot genera unele erori. Pentru sistemul de operare Windows NT sau Windows 2000, numele implicit al directorului de instalare este *WINNT*.

Pasul 23 - Adăugarea unei imprimante de rețea

Această opțiune se personalizează numai în cazul în care dispuneți de un astfel de dispozitiv. Recomandăm însă o altă metodă, care va fi tratată detaliat într-un capitol viitor.

Pasul 24 - Adăugarea unei aplicații care să ruleze după terminarea instalării

Într-una dintre etapele anterioare se vorbea de un auto log-on. Comenzile care se pot specifica în etapa curentă sînt complementare operațiunii anterioare.

Comenzile care se pot folosi cu precădere în această etapă sînt cele de genul instalării unui ServicePack sau instalarea automată a unor aplicații.

Alte comenzi pot fi specificate și la următorul, de altfel și ultimul pas din această etapă.

În exemplul nostru nu vom specifica nici o comandă care va fi executată ulterior.

Mult așteptatul buton **Finish**, și după cum vă așteptați, o altă fereastră care ne informează despre numele viitorului fișier de răspunsuri : *unattend.txt*. Puteți schimba numele acestui fișier (fig. 13.5.9).

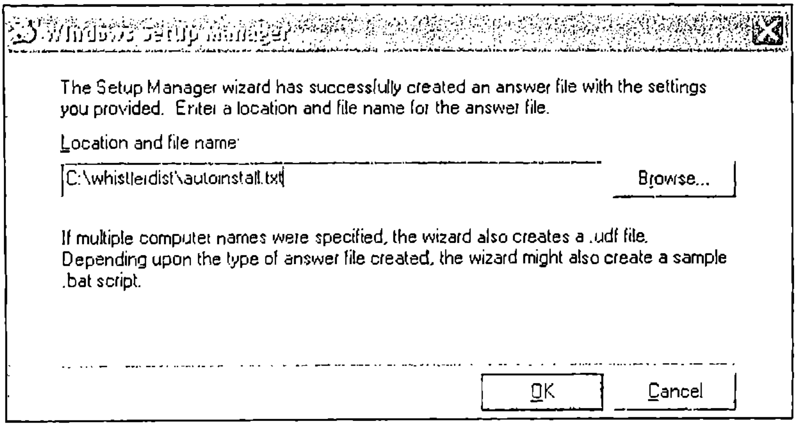


Figura 13.5.9. Etapa finală. Stabilirea numelui fișierului de răspunsuri.

Dacă la pasul 14 au fost specificate mai multe nume de fişiere, se va crea automat un fişier cu acelaşi nume specificat în imaginea anterioară, dar cu extensia UDF, care conţine numele şi datele de personalizare pentru fiecare staţie de lucru. De asemenea, se creează şi un fişier de comenzi (*batch script*) care va fi utilizat pentru instalare.

Pasul 25 - Copierea fişierelor

Reprezintă o etapă a cărei durată depinde de viteza de citire a CD-ului d-voastră. În medie, la un CD de 50x această etapă durează între 7 şi 15 minute.

După terminarea copierii, surprinzător, nu apare nici un buton de final sau confirmare. Închideţi aşadar aplicaţia din **File**, **Exit** şi vizualizaţi conţinutul directorului pe care l-aţi specificat la *pasul 8*. Pe lîngă cele 3 fişiere (*autoinstall.txt*, *autoinstall.bat* şi *autoinstall.udb*) există şi un director cu numele *I386* în care sînt găzduite fişierele destinate instalării. Menţionam anterior că există un fişier *UDF*, dar se pare că în Windows XP extensia acestuia este *UDB*.

Pentru a fi siguri că fişierele create sînt în concordanţă cu cerinţele d-voastră de instalare automată a sistemelor de operare XP, trebuie să realizaţi o serie de modificări în fişierul *autoinstall.txt*. Prezentăm în listing-ul 13.5.1 script-ul original, iar completările sînt scrise cu caractere îngroşate. Comentariile sînt marcate cu bandă, ele netrebuind să apară în viitorul fişier.

Listing-ul 13.5.1. Fişierul *autoinstall.txt* cu completările de rigoare

```
;SetupMgrTag
[Data]
    AutoPartition=1
    MsDosInitiated="0"
    UnattendedInstall="Yes"

[Unattended]
    UnattendMode=FullUnattended
    FileSystem=ConvertNTFS
```

Sistemul de fişiere NTFS reprezintă o condiţie esenţială pentru asigurarea unei politici de securitate la nivel de directoare şi fişiere pe viitoarea staţie de lucru.

```
    OemSkipEula=Yes
    OemPreinstall=Yes
    TargetPath=\WINDOWS

[GuiUnattended]

AdminPassword=4ae7293545151bc4aad3b435b51404eeabe2f97298871
ee70c0a238da505e18f
    EncryptedAdminPassword=Yes
    AutoLogon=Yes
    AutoLogonCount=1
    OEMSkipRegional=1
    TimeZone=115
```

```
    OemSkipWelcome=1

[UserData]
    ProductID= WXP02-XPW01-PXW00-FF001-001FF
    FullName="Admin"
    OrgName="FEAA"
    ComputerName=*

[Display]
    BitsPerPel=32
    Xresolution=1024
    YResolution=768
    Vrefresh=75

[RegionalSettings]
    LanguageGroup=2,1

[SetupMgr]
    ComputerName0=Conta-01
    ComputerName1=Conta-02
    ComputerName2=Market-01
    DistFolder=C:\whistlerdist
    DistShare=whistlerdist

[FavoritesEx]
    Title1="Situatia scolara.url"
    URL1="https://gescoweb.uaic.ro/"
    Title2="E-mail.url"
    URL2="http://webmail.es.uaic.ro/horde/"

[Branding]
    BrandIEUsingUnattended=Yes

[URL]
    Home_Page=http://www.feaa.uaic.ro
    Search_Page=http://www.google.com

[Proxy]
    Proxy_Enable=0
  Use_Same_Proxy=0
```

Opțiunea implicită este 1.

```
[Identification]
    JoinDomain=AlfaSystem
    DomainAdmin=Administrator
```

```
    DomainAdminPassword=parola adminului de domeniu

[Networking]
    InstallDefaultComponents=No

[NetAdapters]
    Adapter1=params.Adapter1

[params.Adapter1]
    INFID=*

[NetClients]
    MS_MSClient=params.MS_MSClient

[NetServices]
    MS_SERVER=params.MS_SERVER

[NetProtocols]
    MS_TCPIP=params.MS_TCPIP

[params.MS_TCPIP]
    DNS=No
    UseDomainNameDevolution=No
    EnableLMHosts=Yes
    AdapterSections=params.MS_TCPIP.Adapter1

[params.MS_TCPIP.Adapter1]
    SpecificTo=Adapter1
    DHCP=No
    IPAddress=172.17.13.25
```

Această linie va fi eliminată urmînd a fi extrasă ulterior din fişierul UDB.

```
    SubnetMask=255.255.255.0
    DefaultGateway=172.17.13.254
    DNSServerSearchOrder=172.172.172.1,172.172.172.2
    WINS=No
    NetBIOSOptions=0
```

Listing-ul 13.5.2. Fişierul *autoinstall.udb* cu completările de rigoare

```
;SetupMgrTag
[UniqueIds]
    Conta-01=UserData,params.MS_TCPIP.Adapter1
    Conta-02=UserData,params.MS_TCPIP.Adapter1
    Market-01=UserData,params.MS_TCPIP.Adapter1
```

Completările au fost efectuate pentru extragerea automată a IP-urilor specificate în lista de mai jos.

```
[Conta-01:UserData]
    ComputerName=Conta-01

[Conta-02:UserData]
    ComputerName=Conta-02

[Market-01:UserData]
    ComputerName=Market-01

[Conta-01:params.MS_TCPIP.Adapter1]
    IPAddress=172.172.172.25

[Conta-02:params.MS_TCPIP.Adapter1]
    IPAddress=172.172.172.26

[Market-01:params.MS_TCPIP.Adapter1]
    IPAddress=172.172.172.27
```

Lista IP-urilor specifice fiecărei stații de lucru:

Listing-ul 13.5.3. Fişierul autoinstall.bat din fericire fără nici o completare

```
@rem SetupMgrTag
@echo off

rem
rem This is a SAMPLE batch script generated by the Setup
rem  Manager Wizard.
rem If this script is moved from the location where it was
rem generated, it may have rem to be modified.
rem

set AnswerFile=.\autoinstall.txt
set UdfFile=.\autoinstall.udb
set ComputerName=%1
set SetupFiles=\\SERVER-01\whistlerdist\I386

if "%ComputerName%" == "" goto USAGE

\\server-01\whistlerdist\I386\winnt32 /s:%SetupFiles% /
unattend:%AnswerFile% /udb:%ComputerName%,%UdfFile% /
makelocalsource /copysource:lang
goto DONE

:USAGE
echo.
```

```
echo Usage: unattend ^<computername^>
echo.

:DONE
```

Server-01 reprezintă denumirea serverului pe care a fost creat punctul de distribuţie.

Textul subliniat din listing-ul 13.5.3 specifică faptul că el trebuie să se încadreze într-o singură linie.

Instalarea propriu-zisă

Etapele instalării sînt:

- formatarea staţiei de lucru;
- crearea unei dischete de bootare prin reţea;
- lansarea în execuţie a fişierului de comenzi *autoinstall.bat* cu parametrul corespondent numelui staţiei care va fi instalată.

Avînd în vedere că instalarea va avea loc pe o maşină fără sistem de operare şi că punctul de distribuţie se află pe o maşină în reţea, avem nevoie de o metodă de accesare a acelui punct de distribuţie.

Pentru aceasta vom folosi un disk bootabil cu acces la reţea (TCP/IP).

Cea mai facilă metodă de a intra în posesia unei astfel de dischete este downloadarea unei imagini de disk bootabil de la www.bovistech.com şi modificarea după preferinţe a acesteia sau crearea cu ajutorul utilitarului *Client Network Administrator* al vechiului sistem de operare Windows NT 4.0 Server.

Dacă optăm pentru a doua variantă, imaginea dischetei trebuie creată după următoarea metodă:

- formatarea cu opţiunea copiere sistem de pe un calculator Windows 9x (*format a : /s*);
- lansarea în execuţie pe un server Windows NT 4.0 a utilitarului *Client Network Administrator*, care conduce la copierea driverelor pentru adapterul de reţea şi a componentelor necesare pentru a porni serviciul de reţea. În cazul în care adapterul maşinii nu este inclus în HCL (*Hardware Compatibility List*), recomandăm folosirea un driver generic *NE2000 Compatible*; pentru a putea folosi această metodă este necesară utilizarea driverelor pentru MS-DOS ale adapterului de reţea respectiv (fişierele au extensia **.dos* şi **.nif*).

Pentru exemplificare, vom considera o dischetă creată pentru driver *NE2000 Compatible* şi dorim să operăm cu această dischetă pe un sistem cu *Realteck 8139*. Driverele MS-DOS pentru acest tip de placă sînt formate din fişierele: *rtsnd.dos* şi *rtsnd.nif*.

Fişierele care trebuie modificate de pe dischetă sînt *protocol.ini*, *system.ini*.

Modificările din *protocol.ini* se vor face în secţiunea:

```
[ms$ne2clone]
```

Numele secţiunii depinde de tipul driverului ales, în cazul nostru NE2000.

```
DriverName = rtsnd$
```

rtsnd$ provine de la numele fişierului driverului de DOS.

Tot în acest fişier se modifică configurația din secțiunea [tcpip]

```
[tcpip]
NBSessions=6
DefaultGateway0=172 172 172 254
SubNetMask0=255 255 255 0
IPAddress0= 172 172 172 250
DisableDHCP=1
DriverName=TCPIP$
BINDINGS=ms$ne2clone
LANABASE=0
```

Modificările din *system.ini*

```
[network drivers]
netcard=rtsnd.dos
```

numele fişierului driverului

```
transport=tcpdrv.dos,nemm.dos
devdir=A:\NET
LoadRMDrivers=yes
```

Totodată se pot modifica valorile parametrilor *computername* şi *username* de la secțiunea [*network*].

```
[network]
filesharing=no
printsharing=no
autologon=yes
computername=Install10
```

numele netbios al stației care se instalează

```
lanroot=A:\NET
username=adminst
```

Utilizatorul cu acces la punctul de distribuție

```
workgroup=Install
reconnect=no
dospophotkey=N
lmlogon=0
logondomain=0
preferredredir=full
autostart=full
maxconnections=8
```

O altă metodă de creare a dischetei este reprezentată de folosirea utilitarelor oferite de aplicații gen *PowerQuest Deploy Center*, care facilitează folosirea unor plăci de rețea cu drivere neincluse în kit-ul Windows NT 4.0.

Pentru accesul în rețea este, de asemenea, necesară existența unui utilizator de domeniu cu ajutorul căruia se va efectua operațiunea de mapare a punctului de distribuție.

Această dischetă este universal valabilă pentru toate staţiile care au acelaşi tip de placă de reţea. Utilizarea unei singure dischete pentru instalarea mai multor sisteme concomitent necesită modificarea, în prealabil, a fişierelor *sistem.ini* şi *protocol.ini* (valorile pentru numele NetBIOS, respectiv adresa IP).

Ţinînd cont de faptul că accesul la punctul de distribuţie este necesar pentru fiecare instalare, se poate mapa *share*-ul din reţea automat, adăugîndu-se comanda **net use** ca ultimă instrucţiune a fişierului *autoexec.bat*.

Specificaţii detaliate privind crearea unei dischete de acces la reţea puteţi găsi la adresa: http://www.microsoft.com/technet/itsolutions/network/deploy/confeat/ tcpboot.asp.

Instalarea efectivă

Presupune bootarea cu discheta de reţea, după formatarea prealabilă a sistemului şi lansarea în execuţie a script-ului creat în punctul de distribuţie (listing 13.5.3), asemănător comenzii specificate în exemplul nr. 1.

Exemplul nr. 1. Comanda de lansare în execuţie a instalării

```
z:\>autoinstall Conta-01
```

Z: reprezintă indicativul discului care a fost mapat de pe serverul din reţea prin comanda **net use z: \\server-01\whistlerdist** specificată în fişierul *autoexec.bat* de pe discheta de conectare la reţea (vezi explicaţiile următoare).

După pornirea instalării, se poate trece la următoarea staţie.

Cu toate că pare una dintre cele mai simple şi lipsite de importanţă operaţiuni, formatarea clasică, folosind discheta de start-up Windows, necesită un timp de lucru cu peste 90% mai mare, în comparaţie cu metoda utilizării unei aplicaţii dedicate, oferită de producătorul HDD-ului respectiv (de exemplu, Seagate Disk Manager, Quantum Disk Manager).

În acest caz, într-o reţea cu lăţimea de bandă de 100mbps instalarea unei singure staţii, inclusiv ultimul service pack, durează aproximativ 40 minute, prezenţa inginerului de sistem fiind necesară timp de 2 minute.

Concluzie

Desigur, dacă nu doriţi să parcurgeţi toţi aceşti paşi pentru a vă crea punctul de distribuţie necesar instalării automate, puteţi să copiaţi conţinutul directorului I386 de pe CD-ul de instalare într-un director local, copiaţi listing-urile 1, 2 şi 3 din acest material, personalizaţi-le după necesităţile d-voastră, puneţi la dispoziţie în reţea directorul respectiv printr-o operaţiune de sharing, copiaţi imaginea dischetei de bootare prin reţea de la adresa: http://www.feaa.uaic.ro/publicatii/retele.htm.

Alte metode de automatizare a instalării

O altă metodă de instalare a mai multor staţii de lucru este aceea a folosirii unui utilitar pentru clonarea discurilor.

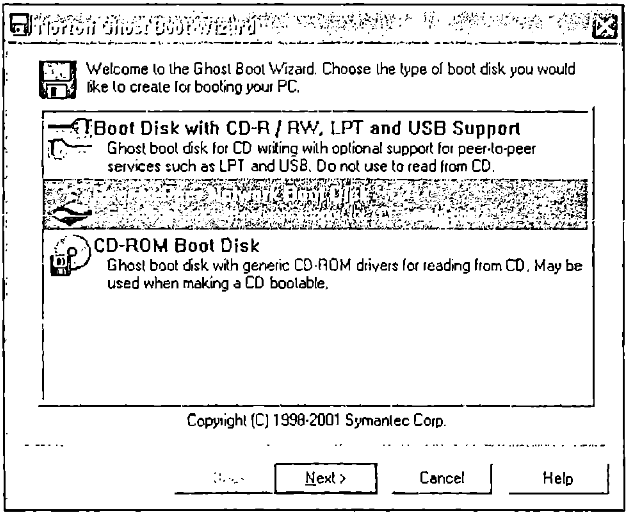


Figura 13.5.10. Utilitarul Norton Ghost Boot Wizard

Un astfel de utilitar este Norton Ghost, actualmente aflat la versiunea 7 și care presupune:

1. Instalarea și configurarea unei stații de lucru.
2. Crearea a două dischete de startare cu posibilitatea de conectare la rețea, folosind utilitarul *Norton Ghost Boot Wizard* (fig. 13.5.10), opțiunea *Peer-to-Peer Network Boot Disk*, care suportă conexiuni TCP/IP.
3. Pornirea stației care va fi clonată cu o dischetă și configurarea acesteia ca *slave*.
4. Pornirea stației de lucru instalate la pasul 1 cu cea de-a doua dischetă și declararea acesteia drept stație *master*, permițînd conectarea la stația slave prin specificarea IP-ului stației *slave*.
5. Preluarea informațiilor de pe stația master pe stația slave (informațiile de pe master vor fi scrise pe discul stației slave).
6. Repornirea sistemelor.
7. Modificarea parametrilor de acces în rețea pentru stația clonată.

Schimbarea configurărilor de rețea

Pentru configurarea parametrilor de conectare la rețea trebuie să parcurgeți următorii pași:

1. RClick **My Network Places** → **Properties**.
2. În fereastra *Network and Dial-up Connections*, RClick pe *Local area connection* → **Properties**.
3. În *Local Area Connection Properties* → **Internet Protocol (TCP/IP)** → **Properties**.
4. În *Internet Protocol (TCP/IP) Properties* → **Use the following IP address**.
5. Scrieți adresa IP, subnet mask și default gateway (dacă este nevoie) → **OK**.

Verificarea conexiunii în reţea

După configurarea proprietăţilor TCP/IP, utilizaţi comenzile **ipconfig** şi **ping** pentru a testa configuraţia locală şi a vă asigura că sistemul d-voastră comunică cu alte sisteme din reţea, utilizînd protocolul TCP/IP.

Secvenţa de comenzi este dată în lista de mai jos:

1. *Ipconfig* – pentru afişarea parametrilor TCP/IP;
2. *ping* localhost – pentru a verifica dacă au fost corect instalate driverele pentru placa de reţea. Această comandă poate afişa şi mesaje de avertizare privind cablul de reţea, în cazul în care acesta nu este conectat;
3. *ping* adresa locală (de exemplu, ping 172.172.72.25);
4. *ping* gateway – pentru a verifica conexiunea către aceasta;
5. *ping* către o alta adresă – pentru a verifica dacă informaţiile sînt duse mai departe de gateway (de exemplu, ping www.siteweb.com).

Adăugarea unei staţii în domeniu în momentul în care aceasta era în prealabil instalată

Pentru a putea adăuga o staţie într-un domeniu Windows, prima adresă de DNS din configurările TCP/IP trebuie să fie adresa serverului DNS din reţeaua la care se doreşte aderarea.

Pentru schimbarea adresei (în Windows XP):

Start → Control Panel → Network and Internet Connections → RClick pe **Network Connections → Properties → Internet Protocol (TCP/IP) → Properties →** *Preferred DNS Server* (se completează adresa serverului de DNS care în cazul nostru este aceeaşi cu adresa serverului de autentificare: 172.172.172.1) **→ OK → OK.**

Pentru adăugarea staţiei în domeniu (în Windows XP):

Start → RClick (pe *My Computer*) **→ Properties → Computer Name → Change →** la Domain se trece numele de NetBIOS al domeniului (în exemplul nostru, *MYDOM*) **→ OK →** în fereastra *Computer Name Change* se trece la *User name*, numele unui administrator de domeniu şi la *Password* parola acestuia... se aşteaptă..., iar în momentul în care se afişează fereastra de informare *Computer Name Changes* cu mesajul *Welcome to the MYDOM domain*, înseamnă că aţi reuşit! Reporniţi sistemul trecînd prin mai multe ferestre de informare.

Mesaje de eroare la adăugarea în domeniu

1. *Numele domeniului*

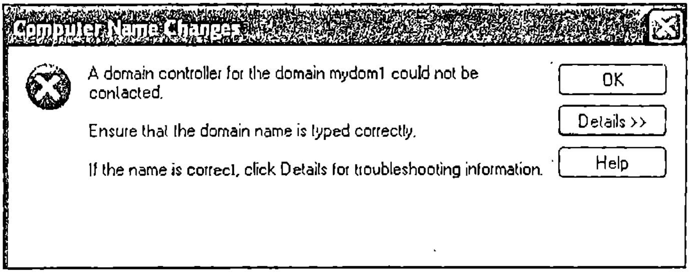


Figura 13.5.11. Probleme cu numele domeniului

În acest caz, numele domeniului nu a fost specificat corect. Aceeaşi eroare poate apărea din lipsa de comunicare dintre server şi staţie; specificarea adreselor de DNS diferite între staţie şi serverul de autentificare.

2. *Dreptul de acces*

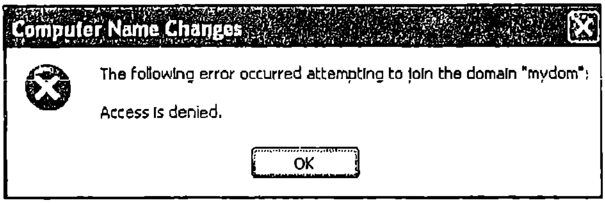


Figura 13.5.12. Mesaj de eroare privind accesul la resursele domeniului

Utilizatorul care s-a specificat în fereastra de autentificare la domeniu nu are dreptul de a adăuga staţii în domeniu. Dacă utilizatorul d-voastră nu aparţine grupului Administrators, atunci staţia nu va putea fi adăugată în domeniu.

3. *Probleme de autentificare*

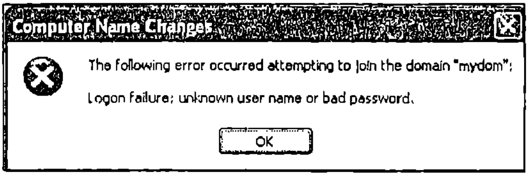


Figura 13.5.13. Probleme cu numele de utilizator sau parola

Eroare cauzată de specificarea greşită a numelui de utilizator sau a parolei de acces în reţea.

După repornire, la fereastra de *Log On to Windows*, dacă apăsaţi pe butonul **Options**, veţi remarca o nouă listă de opţiuni *Log on to*:

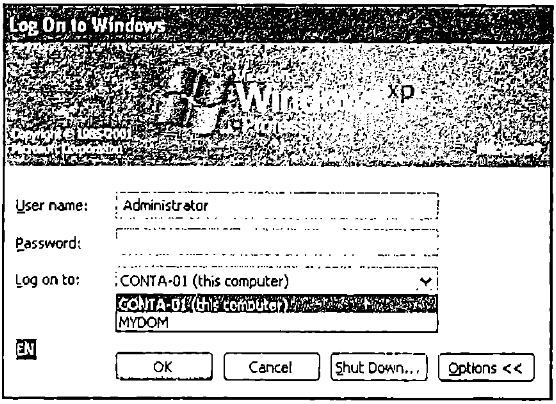


Figura 13.5.14. Fereastra de autentificare care conţine pe lîngă numele staţie de lucru şi numele de NetBIOS al domeniului

Aşadar, chiar dacă o staţie este conectată la un domeniu, utilizatorii locali se pot autentifica în continuare la staţia de lucru. Dacă nu există nici un utilizator creat local, atunci pe această staţie nu se vor mai putea conecta decît utilizatorii din domeniu, (în cazul nostru) *MYDOM* sau utilizatorul local *Administrator* de pe fiecare staţie Windows. Conectarea locală (pe staţie) limitează utilizatorilor accesul la resursele serverului.

Dacă, după ce aţi introdus corect datele de autentificare în reţea, primiţi mesajul:

Figura 13.5.15. Mesaj de eroare cu privire la faptul că domeniul nu este disponibil în momentul respectiv

înseamnă că puteţi să vă încadraţi în una din următoarele situaţii:

- serverul de autentificare nu este pornit;
- cablul de conectare la reţea are probleme (cel mai întîlnit caz, deconectarea din placa de reţea a staţiei de lucru, de obicei cînd personalul administrativ privind curăţenia, în exces de zel, trage puţin mai tare de unitate pentru a şterge praful);
- probleme cu dispozitivele de interconectare în reţea;
- probleme cu serverul de DNS.

Rezolvarea problemelor de genul acesta constă în conectarea cu utilizatorul Administrator (de pe staţia de lucru) şi testarea conexiunii între serverul de autentificare şi staţie.

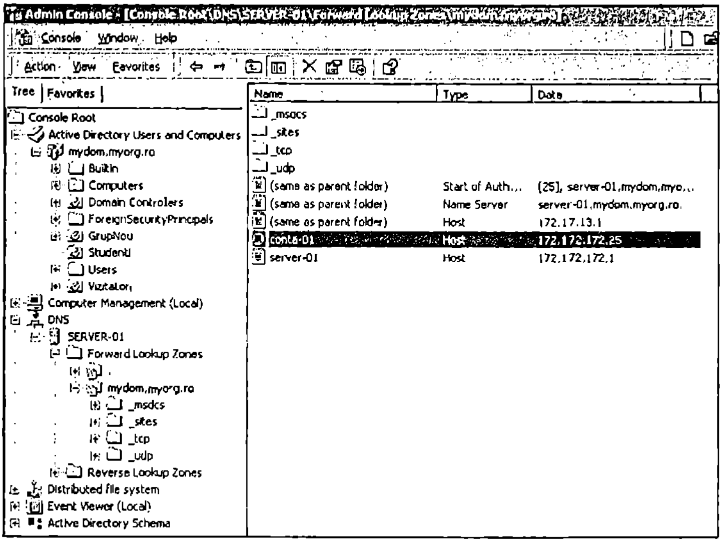


Figura 13.5.16. Consola administrativă în care se observă informaţii despre serviciul DNS

După repornire, pe serverul de DNS apare automat o nouă înregistrare aferentă noii stații de lucru. O stație de lucru poate avea mai multe nume specificate în DNS (fig. 13.5.16).

13.6. Configurarea Active Directory. Crearea utilizatorilor. Definirea politicilor de securitate

Una dintre etapele esențiale în definirea unui domeniu W2k este reprezentată de crearea conturilor de utilizator, organizarea acestora pe grupuri organizaționale și crearea unei politicii de securitate pentru aceștia.

Lansarea Active Directory în scopul configurării : **Start → Programs → Administrative Tools → Active Directory Users and Computers.**

Vă recomandăm, în schimb, să vă creați o consolă administrativă în care să includeți mai multe componente de administrare pentru serverul d-voastră :

1. **Start → Run → MMC ;**
2. **Meniul Console → Add/Remove Snap-in → Add → Active Directory Users and Computers → Add → Computer Management → Add → Finish → DNS → Add → Event Viewer → Add → Finish → Distributed file system → Event Viewer → Add → Finish → Close.**

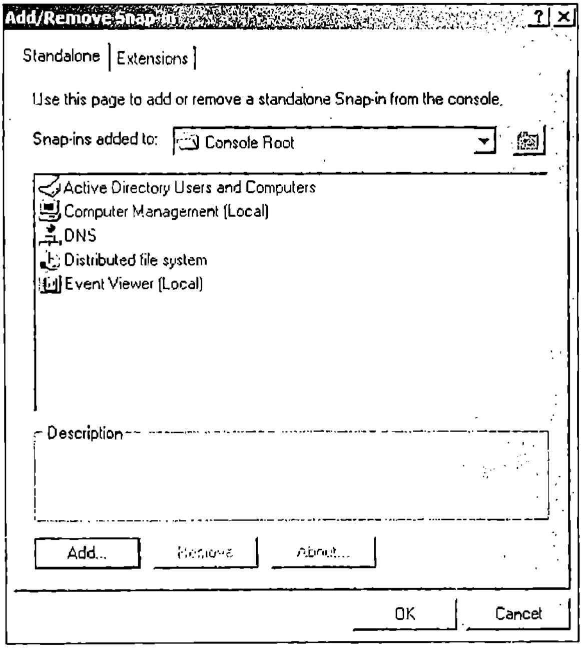


Figura 13.6.1. Adăugarea extensiilor într-o consolă administrativă

Pentru configurarea extensiilor pentru fiecare categorie în parte din fereastra *AddRemove Snap-in* (fig. 13.6.1), alegeţi tab-ul **Extensions**, dezactivaţi *Add all extensions* şi păstraţi numai opţiunea *Group Policy*, după care alegeţi din listă următoarea componentă: *Computer Management*, dezactivaţi *Add all extension* şi alegeţi opţiunile care vă interesează pentru fiecare categorie în parte.

După ce confirmaţi, puteţi salva consola administrativă pentru utilizări ulterioare din meniul **Console**, opţiunea **Save**. Vă recomandăm să o salvaţi pe desktop-ul sistemului d-voastră pentru a fi accesibilă cît mai uşor.

Notă: Această opţiune de creare a consolei administrative nu este obligatorie.

Scurtă prezentare a componentei Active Directory Users and Computers (A.D.U.C.)

A.D.U.C. pentru domeniul curent conţine, în mod implicit, 5 categorii:

- *Builtin* – care conţine un set de utilizatori predefiniţi cu diferite roluri în cadrul domeniului d-voastră.
- *Computers* – conţine toate staţiile incluse în domeniul curent.
- *Domain Controllers* – include toate serverele din domeniul curent care au instalat şi configurat serviciul A.D.
- *ForeignSecurityPrincipals* – conţine identificatorii de securitate (security identifiers – SIDs) asociaţi obiectelor A.D. din alte domenii decît cel curent.
- *Users* – conţine informaţii despre toţi utilizatorii şi grupurile de utilizatori implicite.

A.D.U.C. poate gestiona informaţii despre calculatoare, grupuri de utilizatori, grupuri organizaţionale, imprimante, utilizatori şi directoare puse la dispoziţie în reţea (*shared folder*).

Înainte de crearea unui utilizator vă recomandăm să creaţi întîi un nou grup organizaţional care poate include şi staţii de lucru, şi asupra căruia se poate crea o politică de securitate centralizată: **Action** → **New** → **Organizational Unit** → introduce-ţi o denumire sugestivă, (de exemplu, Vizitatori) → **OK**.

La proprietăţile unui grup organizaţional putem specifica următoarele informaţii:

- informaţii generale (*General*). Conţine informaţii privind descrierea grupului şi adresa la care poate fi localizat acesta;
- informaţii despre persoana, utilizatorul care gestionează grupul respectiv (*Managed By*). Persoana care se ocupă de gestiunea utilizatorului respectiv poate fi schimbată apăsînd butonul **Change**, datele de identificare despre aceasta fiind preluate automat din A.D.;
- politicile de securitate aplicate grupului respectiv (*Group Policy*) unde avem posibilitatea de creare a unei noi politici de securitate sau importul unei politici deja existente. Nu activaţi opţiunea *Block Policy inheritance* pentru că aceasta nu se va mai propaga automat asupra altor subsisteme organizaţionale din grupul respectiv.

Crearea unei noi politici de securitate şi cîteva aspecte şi motivaţii ale unei politici de securitate

Din A.D.U.C., RClick (pe grupul organizaţional) → **Properties** → **Group Policy** → **New** → (se tastează numele politicii, de exemplu, vizPol - politica pentru vizitatori) → **Edit**.

Fereastra *Group Policy* este împărţită în două mari categorii:

- *Computer Configuration* (politica staţiilor de lucru şi a serverelor din domeniu);
- *User Configuration* (politica de securitate pentru utilizatorii din grupul organizaţional respectiv).

Dacă un grup organizaţional conţine numai utilizatori sau numai calculatoare, cealaltă opţiune poate fi blocată din fereastra de proprietăţi a politicii de securitate (RClick [pe numele politicii] → **Properties**) (fig. 13.6.2).

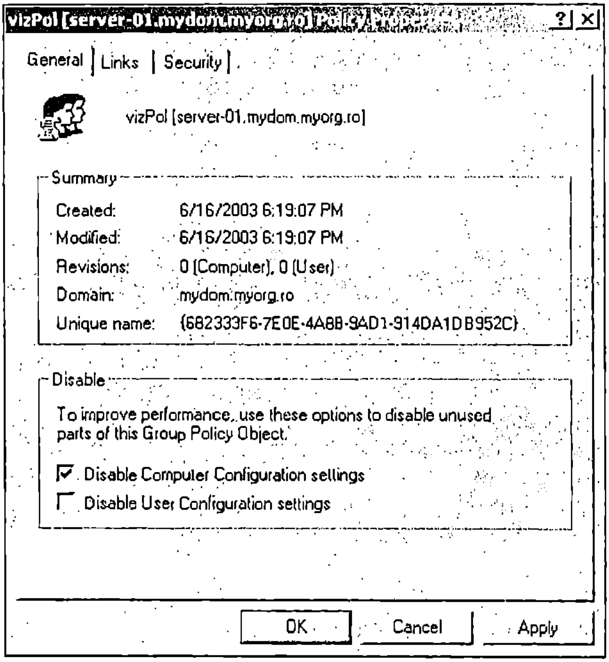


Figura 13.6.2. Proprietăţile politicii de securitate

În momentul în care activaţi una dintre cele 2 opţiuni, va apărea pe ecranul d-voastră o fereastră de atenţionare cu privire la consecinţele care pot fi generate în urma acestei operaţiuni, respectiv faptul că staţiilor de lucru din acest grup organizaţional le va fi aplicată politica de securitate locală. Apăsaţi cu încredere butonul **Yes**, pentru că se poate reveni în orice moment la starea iniţială.

Vă recomandăm să creaţi o politică de securitate cu preponderenţă orientată spre utilizator, pentru că pe aceeaşi staţie se pot conecta diferite categorii de utilizatori care

pot avea diferite niveluri de acces la aceasta, anumite operaţiuni fiindu-le private de o eventuală politică de securitate eronat specificată.

O primă subcategorie întîlnită la ambele categorii este *Software Settings* ce conţine opţiunea *Software installation*, care presupune instalarea automată a unor aplicaţii împachetate în prealabil în mod administrativ. Pachetele utilizate în acest scop sînt recunoscute sub extensia *MSI*. Cîteva instrumente folosite pentru crearea pachetelor de instalare MSI sînt: *Veritas Software Console*, *InstallShield Professional*, *Wise Package Studio*. Aceste pachete se salvează într-un director pus la dispoziţie în reţea. Instrumentele respective se bazează pe crearea unei imagini (*snapshot*) a regiştrilor sistemului de operare, instalarea şi configurarea aplicaţiilor, repornirea sistemului, împachetarea aplicaţiei prin preluarea fişierelor de pe disc, precum şi a cheilor introduse în regiştri. Din testele pe care le-am efectuat cu *Veritas Software Console*, acest sistem se aplică cu succes doar aplicaţiilor de mici dimensiuni, gen arhivare.

În subcategoria *Windows Settings* există opţiunea *Scripts* care pentru *Computer Configuration* include subopţiunile *Startup* şi *Shutdown*, iar la *User Configuration* include *Log on* şi *Log off*. Aici se pot specifica diferite script-uri care să se declanşeze în momentul în care staţia sau utilizatorul se autentifică în reţea. Asupra cîtorva modele de script-uri vom reveni ulterior.

O opţiune din politica de securitate poate avea 3 stări:

- Nedefinită/neconfigurată (not defined/not configured);
- Definită/Activă (specificarea unei valori/Enabled);
- Indisponibilă (Disabled).

Schimbarea valorilor se poate realiza prin acţionarea dublu Click pe opţiune sau din meniul **Action**, opţiunea **Security**.

În continuare, vom încerca să explicăm cîteva dintre opţiunile politicii uzuale de securitate, valorile aferente şi, înainte de toate, calea de a ajunge la opţiunea respectivă.

Computer Configuration\ Windows Settings\ Security Settings\ Account Policies\ Password Policies:

- *Maximum password age* (durata maximă de valabilitate a unei parole) – forţează utilizatorul ca după un anumit număr de zile (implicit 70) să-şi schimbe parola. Este în strînsă legătură cu *Minimum Password age* (durata minimă de valabilitate a unei parole) (implicit 30 de zile).
- *Passwords must meet complexity requirements* (parola trebuie să aibă un format complex) – care înseamnă că aceasta nu trebuie să conţină o parte sau tot numele de utilizator; să nu fie mai mică de 6 caractere; să conţină caractere mari, mici, numere şi caractere non-alfanumerice (de exemplu, !, $—›, %). De asemenea, se recomandă folosirea caracterelor speciale sau a caracterului spaţiu în crearea parolelor. Activarea acestei opţiuni forţează utilizatorul să nu mai folosească data naşterii, numărul de la maşină sau nume familiare în crearea parolelor.

Computer Configuration\ Windows Settings\ Security Settings\ Account Policies\ Account Lockout Policy:

- *Account lockout threshold* (blocarea contului de utilizator) – se configurează pentru a preveni încercările repetate de conectare la reţea în condiţiile de necunoaştere

a parolei. Valorile pe care le poate lua sînt de la 1 la 999. Implicit această opțiune nu este configurată, iar valoarea 0 elimină posibilitatea de blocare a contului. Recomandăm valoarea 3 pentru această opțiune.

- *Account lockout duration* (timpul de blocare a unui cont) – specifică durata de blocare a unui cont care a fost blocat automat prin opțiunea anterioară. Intervalul de valori este cuprins între 1 și 99999 minute, valoarea implicită fiind de 30 de minute, configurabilă automat în momentul în care se configurează opțiunea anterioară.

Computer Configuration\ Windows Settings\ Security Settings\ Local Policies\ Audit Policy:

- *Audit account log-on events* (înregistrarea evenimentelor de conectare în rețea) – permite scrierea unei înregistrări în *Event Viewer* pentru fiecare operațiune de *log in* sau *log off* pe care o efectuează un utilizator autentificat de o stație din domeniu. În strînsă legătură cu aceasta este opțiunea *Audit logon events*.
- *Audit account management* (înregistrarea evenimentelor de modificare a conturilor de utilizator) – opțiune foarte utilă în gestiunea unei rețele, fiind foarte important de știut cînd și de către cine au fost efectuate modificări asupra conturilor de utilizatori.
- *Audit policy change* (înregistrarea schimbărilor politicii de securitate) – adaugă în *Event Viewer* înregistrări despre modificările drepturilor de acces la anumite resurse pe stația respectivă.

Computer Configuration\ Windows Settings\ Security Settings\ Local Policies\ User Rights Assignment:

- *Add workstations to domain* (adăugarea de stații în domeniu) – se configurează pentru a permite utilizatorilor sau unui grup de utilizatori să adauge stații de lucru în domeniu. Implicit, grupul de utilizatori care poate adăuga stații în domeniu este *Authenticated Users*, dar în această categorie pot intra toți utilizatorii creați în Active Directory, ceea ce diminuează controlul asupra stațiilor din domeniul respectiv. Vă recomandăm să configurați această politică de securitate cu specificarea strictă a grupului Administrators: Dublu Click (pe opțiune) → **Define these policy settings in the template** → **Add** → **Browse** → dublu click (pe Administrators) → **OK** → **OK** → **OK**.
- *Change the system time* (schimbarea timpului din sistem). În mod implicit, fiecare utilizator poate să schimbe data și ora sistemului, dar nu recomandăm acest lucru pentru că poate duce la înregistrarea greșită din punctul de vedere al timpului a unor evenimente din rețea. Schimbați asemănător exemplului anterior această opțiune, definind dreptul de acces grupurilor administrative la nivel de domeniu.

> *Pont*: Sincronizarea timpului de pe stații în mod automat într-o rețea se poate realiza prin comanda *net time* care poate fi specificată într-un script de *startup* pe stațiile din domeniu.
> De exemplu: net time /rtsdomain: nume_domeniu /set.

Computer Configuration\ Windows Settings\ Security Settings\ Local Policies\ Security Options:

- *Additional restrictions for anonymous access* (Acces limitat conexiunilor anonime). Orice utilizator din domeniul curent sau din alte domenii poate vedea, în mod implicit, resursele puse la dispoziţie în reţea. Pentru a oferi o mai bună protecţie domeniului recomandăm opţiunea *Do not allow enumeration of SAM accounts and shares*, care înlocuieşte grupul de utilizatori *Everyone* cu *Authenticated Users* în definirea politicilor locale de acces la diferite resurse. În acest fel, numai utilizatorii din Active Directory pot avea acces la resursele domeniului: share-uri, imprimante etc.
- *Automatically log off users when logon time expires* (Deconectarea automată de la reţea în momentul expirării timpului de lucru). Pentru anumite categorii de utilizatori sau în mod individual poate fi configurat un interval orar de acces în reţea. În momentul în care utilizatorul depăşeşte timpul alocat, acesta este deconectat automat de la resursele reţelelor. De asemenea, şi versiunea următoare (local) trebuie activată pentru ca sistemul să deconecteze automat utilizatorul.
- *Do not display last user name in logon screen* (Neafişarea numelui ultimului utilizator conectat pe staţia curentă). În cazul reţelelor cu mulţi utilizatori, activarea acestei opţiuni aduce un spor de siguranţă la conectarea în reţea, mulţi utilizatori nefiind destul de atenţi la ultimul *User Name* scris în fereastra de *Log On*. În cazul în care într-o reţea acelaşi utilizator lucrează cu preponderenţă pe aceeaşi staţie, activarea acestei opţiuni nu este recomandată.
- *Message text for users attempting to log on* (Mesajul pentru utilizatorii care doresc să se conecteze în reţea). Aici se poate trece un mesaj de informare a utilizatorilor care se conectează în reţea. Opţiunea *Message title for users attempting to log on* specifică titlul ferestrei de mesaj (de exemplu, *Bun venit în cadrul reţelei MYDOM*).
- *Number of previous logons to cache (in case domain controller is not available)* (Numărul conectărilor anterioare salvate local în cazul în care serverul de domeniu nu este disponibil) – permite conectarea pe staţii folosind utilizatorii de domeniu chiar şi în cazul în care serverul de autentificare este temporar indisponibil. Această opţiune este recomandabilă numai în cazul în care domeniul conţine puţini utilizatori, şi aceştia se conectează cu precădere pe aceeaşi staţie. În cazul domeniilor cu mulţi utilizatori, crearea profilurilor de utilizatori locali duce la o diminuare a spaţiului disponibil pe disc. Valoarea *0* este corespondentă cazului al doilea.
- *Prompt user to change password before expiration* (Atenţionarea utilizatorului pentru a-şi schimba parola cu un anumit timp înainte de expirare). Se exprimă în zile, valoarea implicită fiind 14. Vă recomandăm însă o valoare mai mică, 5 sau 7, pentru a nu deranja utilizatorul la fiecare conectare. Schimbarea parolei acestuia duce la anularea apariţiei mesajului de avertizare pînă la următorul termen.
- *Restrict CD-ROM access to locally logged-on user only* (Blocarea accesului la CD-ROM utilizatorilor autentificaţi de staţie şi nu de serverul de domeniu). Se utilizează pentru prevenirea instalării unor aplicaţii, copierii de fişiere etc. de alţi utilizatori decît cei autentificaţi în domeniu. De asemenea, se poate interzice accesul către unitatea de dischetă prin următoarea opţiune: *Restrict floppy access to locally logged-on user only*.

Computer Configuration\ Windows Settings\ Security Settings\ Event Log\ Settings for Event Logs :

În această secțiune, activarea opțiunilor *Retain application, system, security log* și configurarea lor la un anumit număr de zile (implicit 7) aduce cu sine o configurare automată a opțiunilor *Retention method for...* care pot fi configurate implicit pe zile.

Computer Configuration\ Windows Settings\ Security Settings\ Restricted Groups este destinată limitării drepturilor anumitor grupuri de utilizatori, prin adăugarea acestora în această categorie : RClick pe opțiune → **Add Group** → **Browse** → se alege grupul din listă → **OK** → **OK**.

Computer Configuration\ Windows Settings\ Security Settings\ System Services este destinat configurării serviciilor care vor rula pe stațiile de lucru din domeniu. Se pot defini modul de pornire a serviciului, precum și grupurile de utilizatori care au dreptul de pornire a respectivului serviciu. De exemplu, dorim ca serviciul Telnet să pornească manual și numai administratorul de domeniu să aibă drepturi de execuție asupra acestuia : Dublu Click pe serviciu → activați *Define this policy settings in the template* → în fereastra *Security for Telnet* apăsați **Add** → se alege din listă grupul *Administrators* → **OK** → se apasă opțiunea **Allow**, **Full Control** de la *Permissions* → Click pe *Everyone* → **Remove** → **OK** → **Manual** → **OK**. Atenție la modul de pornire a anumitor servicii. Testați în prealabil pe o stație obișnuită care dintre servicii vă pot asigura o funcționalitate optimă și care pot fi oprite. Este bine cunoscut că un număr mai mic de servicii aduce cu sine și o memorie RAM suplimentară.

Computer Configuration\ Windows Settings\ Security Settings\ Registry este opțiunea prin intermediul căreia administratorii pot defini permisiuni de acces utilizatorilor pe anumite secțiuni din regiștrii sistemului de operare de pe stațiile de lucru.

Computer Configuration\ Windows Settings\ Security Settings\ File System permite administratorilor adăugarea și definirea politicii de securitate la nivelul directoarelor și fișierelor de pe stațiile de lucru.

Computer Configuration\ Administrative Templates conține o serie de șabloane de opțiuni predefinite configurabile. Șabloanele implicite sînt *conf*, *inetres*, *system*. Adăugarea unui nou șablon aduce cu sine posibilitatea configurării de noi opțiuni de securitate : RClick (pe Administrative Templates) → **Add/Remove Templates** → **Add** → se alege un cadru din listă (de exemplu, *inetset*) → **Open** → **Close**.

Opțiunile din Administrative Templates sînt foarte multe, o să amintim aici doar cîteva, precizând că o documentare completă a acestora puteți găsi la adresa http://msdn.microsoft. com/library/en-us/gp/default.asp

- Încetarea apariției ferestrei de bun venit la conectarea în rețea : *Computer Configuration\ Administrative Templates\ System\ Don't display welcome screen at logo.*
- Blocarea rulării automate a unui CD în momentul introducerii acestuia în unitatea de CD-ROM : *Computer Configuration\ Administrative Templates\ System\ Disable Autoplay.*

- În cazul în care aveţi mai multe servere de autentificare pentru domeniu, propagarea schimbărilor care se efectuează pe acestea poate fi configurată din: *Computer Configuration\ Administrative Templates\ System\ Group Policy\ Group Policy refresh interval for domain controllers*. Valoarea implicită este de 5 minute.

Prezentarea principalelor categorii din User Configuration

- Personalizarea titlului pentru Internet Explorer şi a imaginii de pe bara cu instrumente: *User Configuration\ Windows Settings\ Internet Explorer Maintenance\ Browser User Interface\ Browser Title* → *Customize Title Bars* → scrieţi textul dorit → *Customize Toolbar background bitmap* → *Browse* → căutaţi imaginea care trebuie să fie de tip bitmap (*.BMP) → *Open* → *OK*.
- Specificarea unui proxy pentru comunicarea pe Internet: *User Configuration\ Windows Settings\ Internet Explorer Maintenance\ Connection\ Proxy Settings* → adăugaţi adresa serverului dorit în lista HTTP, portul de comunicaţie → *OK*;
- Personalizarea paginii de start (*home page*), a paginii de căutare şi a paginii pentru asistenţa tehnică: *User Configuration\ Windows Settings\ Internet Explorer Maintenance\ URLs\ Important URLs* → *Customize Home page\ Search bar\ Online support page URL* → se tastează adresa paginilor dorite → *OK*. Această opţiune este foarte importantă pentru configurarea unei pagini HTML drept desktop al staţiilor din domeniu.
- Pentru specificarea altei locaţii directorului My Documents: *User Configuration\ Windows Settings\ Folder Redirection\ My Documents* → RClick (pe *My Documents*) → *Properties* → *Target* → În lista *Settings* există opţiunea *Basic - Redirect everyone's folder to the same location* (redirectarea tuturor utilizatorilor către aceeaşi locaţie), iar la *Target folder location* treceţi adresa la care va fi redirectat automat directorul *My Documents* pentru fiecare utilizator în parte. Calea pe care v-o recomandăm este \\nume_server\nume_share în cazul nostru adresa fiind \\server-01\%username%$, server-01 fiind numele serverului, iar username fiind variabila sistem care identifică numele de share pentru fiecare utilizator în parte. La opţiunea *Settings* toate opţiunile pot rămîne în mod predefinit. Politica de securitate pentru *My Pictures* este configurată automat să urmeze directorul My Documents (*Follow the My Documents folder*).
- Interzicerea schimbării paginii de start (*home page*): *User Configuration\ Administrative Templates\ Windows Components\ Internet Explorer\ Disable changing home page settings*.
- Ascunderea opţiunii *Folder Option* din meniul *Tools* din Windows Explorer cu scopul de a nu permite utilizatorilor vizualizarea unor fişiere ascunse, sau fişiere sistem, în scop distructiv, sau a eliminării lor din necunoştinţă de cauză: *User Configuration\ Administrative Templates\ Windows Components\ Windows Explorer\ Removes the Folder Option menu item from the Tools menu*. Opţiunea ascunderii fişierelor şi eliminarea posibilităţii de dezascundere poate fi depăşită cu utilitarul *Command Prompt*, comanda *attrib*.
- Ascunderea anumitor discuri în *My Computer*, pentru a restricţiona accesul la acestea: *User Configuration\ Administrative Templates\ Windows Components\ Windows Explorer\ Hide these specified drives in My Computer* → *Enabled* → alegeţi opţiunile dorite din listă → *OK*. Foarte multe erori care se întîmplă în

utilizarea calculatoarelor sînt cauzate de mutarea accidentală prin drag-and-drop a directoarelor dintr-o locație în alta. Pentru protejarea sistemului de operare, dar și pentru a păstra o ordine în organizarea fișierelor de pe discul **C:**, vă recomandăm să activați opțiunea *Restrict C drive only*. De asemenea, puteți bloca accesul la discurile **A:** sau **B:** pentru a vă proteja și prin această cale de utilizatorii care pot transporta viruși pe dischete (*Restrict A, B and C drives only*). În cazul în care doriți blocarea accesului la CD-ROM, trebuie să activați opțiunea *Restrict D drive only*, cu specificarea faptului că trebuie să vă configurați partițiile de pe stațiile de lucru (*Administrative Tools\ Computer Management\ Disk Management*) în așa fel încît discul de CD-ROM să aibă asignată litera **D**. Dacă stația d-voastră face parte dintr-un domeniu public, gen i-cafe, puteți ascunde toate discurile de pe stație, prin activarea opțiunii *Restrict all drives*. Chiar dacă activați această politică de securitate, accesul la discuri este posibil din *Command Prompt* numai dacă nu ați dezactivat această opțiune.

- Eliminarea iconiței *My Network Places* din Windows Explorer pentru a preveni accesul neautorizat în rețea : *User Configuration\ Administrative Templates\ Windows Components\ Windows Explorer\ No „Entire Network" in My Network Places*. Oricît de protejați credem că sîntem, să nu uităm niciodată că un utilizator interesat în scop distructiv se „leagă" de orice informație pe care o achiziționează pentru a-și testa „forțele". Între 50 și 85% dintre incidentele de securitate provin din interiorul organizației[1].
- Specificarea numărului maxim de documente stocate în lista documentelor recent apelate: *User Configuration\ Administrative Templates\ Windows Components\ Windows Explorer\ Maximum number of recent documents* (valoare implicită : 15).
- Eliminarea opțiunii *Run* din meniul *Start*: *User Configuration\ Administrative Templates\ Start Menu & Taskbar \ Remove Run Menu from Start Menu*.
- Ascunderea iconiței de acces la rețea de pe Desktop : *User Configuration\ Administrative Templates\ Desktop\ Hide My Network Places icon on desktop*.
- Interzicerea schimbării destinației directorului sistem My Documents: *User Configuration\ Administrative Templates\ Desktop\ Prohibit user from changing My Documents path*.
- Activarea desktop-ului activ : *User Configuration\ Administrative Templates\ Desktop\ Active Desktop\ Enable Active Desktop* și interzicerea modificărilor : *User Configuration\ Administrative Templates\ Desktop\ Active Desktop\ Prohibit changes*.
- Adăugarea unei pagini Web pe desktop-ul activ: *User Configuration\ Administrative Templates\ Desktop\ Active Desktop\ Add/Delete Item → Enabled →* specificarea adresei unei pagini Web care se dorește a fi postată pe desktop-ul utilizatorilor *→ OK*.
- Ascunderea resursei Active Directory în rețea : *User Configuration\ Administrative Templates\ Desktop\ Active Directory\ Hide Active Directory folder*.
- Interzicerea accesului la tabloul de bord al calculatorului (Control Panel) : *User Configuration\ Administrative Templates\ Control Panel\ Disable Control Panel*.
- Dacă doriți în schimb să păstrați numai anumite componente în Control Panel, puteți alege opțiunea *Show only specified control panel applets* și specificați

1. Oprea, D., *Protecția și securitatea sistemelor informaționale*, Ed. Polirom, Iași, 2002, p. 154.

numele componentelor pe care le doriţi. Pentru a crea o listă de componente: **Show** → **Add** → introduceţi numele componentei → **OK** → **OK**. Componentele pe care le puteţi folosi le găsiţi în directorul în care a fost instalat sistemul de operare, subdirectorul *System32*, sub forma unor fişiere cu extensia *CPL*. Pot exista în schimb şi neclarităţi în legătură cu aceste componente pentru că, de exemplu, nu există nici un *CPL* care să deschidă fereastra de configurare a tastaturii, şi nici a imprimantelor. Dacă în documentaţie se exemplifică pe lîngă mai multe CPL-uri şi Printers, înseamnă că putem încerca opţiunea Keyboard pentru ca iconiţa pentru tastatură să fie singura vizibilă în Control Panel. Nouă nu ne-a funcţionat!

- Interzicerea modificării setărilor pentru display: *User Configuration\ Administrative Templates\ Control Panel\ Display\ Disable Display* în Control Panel. Această regulă poate fi considerată una dintre cele mai drastice pentru utilizatorul final. De ce ar trebui să implementăm o astfel de politică în care utilizatorul să nu-şi poată adăuga drept Wallpaper fotografia unui loc, a unei persoane sau animal drag? Vă prezentăm un caz practic, deosebit de real, concluziile urmînd să le trageţi d-voastră. Într-o onorabilă instituţie de învăţămînt, o onorabilă profesoară de informatică a fost foarte aproape de pragul unui colaps psihic în momentul în care a intrat într-un laborator, desktop-ul fiecărei staţii de lucru fiind schimbat cu fotografii din cea mai exotică zonă a XXX-ului. Folosirea acestei politici de securitate diminuează posibilitatea de apariţie a unor cazuri de acest gen, pentru că în utilitarul *Paint* există încă posibilitatea de setare a unei imagini drept fundal al desktop-ului d-voastră.
- Interzicerea modificării parametrilor TCP/IP: *User Configuration\ Administrative Templates\ Network\ Network and Dial-up Connections\ Allow TCP/IP advanced configuration* → *Disable*.
- Blocarea accesului la utilitarul pentru comenzi (*Command Prompt*): *User Configuration\ Administrative Templates\ System\ Disable the command prompt*. În această secţiune, la opţiunea Enabled foarte important este modul în care se vor executa script-urile. Dacă la procesul de autentificare de reţea aveţi script-uri de tip *BAT* pentru diferite operaţiuni, alegeţi din lista *Disable the command prompt script processing also* opţiunea No.
- Interzicerea accesului la regiştrii sistemului de operare, activaţi opţiunea *Disable registry editing tools*.
- Interzicerea accesului către anumite aplicaţii: *Don't run specified Windows applications* → **Enabled** → **Show** → **Add** → se trece numele aplicaţiei a cărei rulare dorim s-o interzicem, de exemplu, *sol.exe*, aplicaţia pentru jocul *Solitaire*, dar lista aplicaţiilor nu se limitează numai la aplicaţii Windows, ci şi alte executabile gen mIRC32.exe → *OK* → *OK* → *OK*.
- Limitarea accesului la aplicaţia de gestiune a proceselor (*Task Manager*): *User Configuration\ Administrative Templates\ System\ Logon\ Logoff\ Disable Task Manager*; recomandăm această opţiune în momentul în care rulaţi aplicaţii de monitorizare pe staţiile de lucru sub formă de servicii, pentru a preveni oprirea neautorizată a acestora de către utilizatori.

Detalii despre celelalte opţiuni de configurare a politicii de securitate puteţi găsi la adresa specificată într-un paragraf anterior.

În momentul în care închideți fereastra Group Policy, toate configurările pe care le-ați personalizat în această secțiune se salvează automat. De asemenea, trebuie să închideți și fereastra de proprietăți a grupului organizațional.

Crearea conturilor de utilizatori

Se spune că o rețea perfectă este cea fără utilizatori, dar însuși scopul acesteia este de a permite utilizatorilor o comunicare rapidă și o stocare centralizată a fișierelor și aplicațiilor.

Organizarea utilizatorilor în Windows 2000 se face pe grupuri, fiecare grup având anumite drepturi și niveluri de acces la resursele rețelei. Nu trebuie să uităm grupurile organizaționale care asigură o gestiune centralizată a resurselor disponibile.

Crearea unui cont de utilizator în A.D.U.C.

1. RClick (pe numele domeniului) → **New** → **User** → în fereastra New Object - User completați cîmpurile: prenume (*First name*), numele de familie (*Last name*), numele complet (*Full name*) se completează automat, numele de utilizator (*User logon name*) care va fi folosit la conectare; vă recomandăm să nu folosiți spații în numele utilizatorului → **Next**.

2. Introduceți parola utilizatorului și confirmați parola (*Confirm password*), după care puteți activa următoarele opțiuni:

- utilizatorul va fi obligat să-și schimbe parola la prima autentificare în rețea (*User must change password at next logon*); recomandăm această opțiune cu preponderență în rețele cu foarte mulți utilizatori, în care parolele se creează după un anumit algoritm deductibil. Din experiența noastră putem afirma că după conectare utilizatorul se așteaptă să vadă background-ul Windows-ului și nu o fereastră care-l mai întreabă încă o dată ceva despre parola veche (*Old Password*), și una nouă (*New Password*) care trebuie confirmată (*Confirm New Password*) și care mai trebuie să fie și diferită de cea veche;

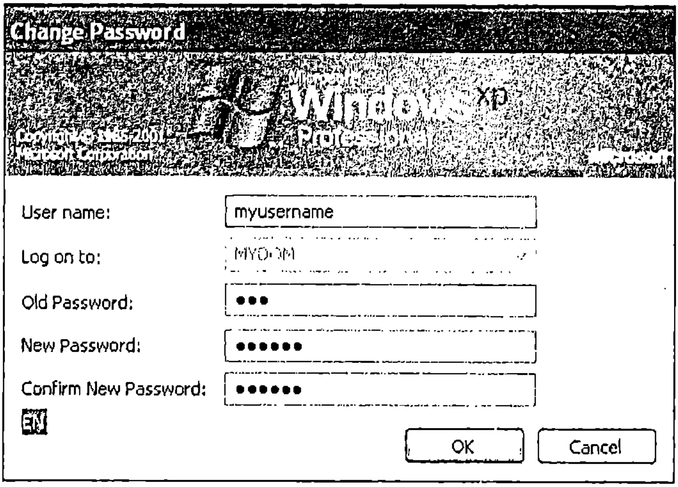


Figura 13.6.3. Fereastra de schimbare a parolei

- utilizatorul nu va putea să-şi schimbe parola (*User cannot change password*) – opţiune pe care o recomandăm în cazul conturilor de utilizator destinate grupurilor de persoane. Schimbarea parolei de către un utilizator duce la imposibilitatea conectării celorlalţi utilizatori la reţea ;
- parola nu va expira niciodată (*Password never expires*), activarea acestei opţiuni lasă la latitudinea utilizatorului politica de gestionare a propriei parole de acces în reţea, ceea ce nu este întotdeauna recomandat ;
- contul va fi inactiv (*Account is disabled*), în cazul în care contul va fi utilizat într-o altă perioadă de timp viitoare celei creării contului.

Neactivarea nici unei opţiuni lasă la latitudinea politicii de securitate aceste opţiuni.

În mod implicit, utilizatorul va fi găsit în categoria Users din A.D.U.C.

La proprietăţile utilizatorului nou creat, vom găsi nu mai puţin de 12 categorii de informaţii foarte detaliate despre utilizatori :

- **General** – se pot configura informaţii despre datele de identificare a utilizatorului în mod electronic : e-mail, Web Page ;
- **Address** – informaţii despre adresa poştală a utilizatorului : strada (*Street*), oraşul (*City*) ;
- **Account** – conţine o serie de informaţii despre numele de utilizator (*User logon name*), cîteva opţiuni suplimentare (*Account options*), durata de valabilitate a contului (*Account expires*).

O secţiune importantă din această categorie este reprezentată de posibilitatea de specificare a unui interval orar de conectare la reţea :

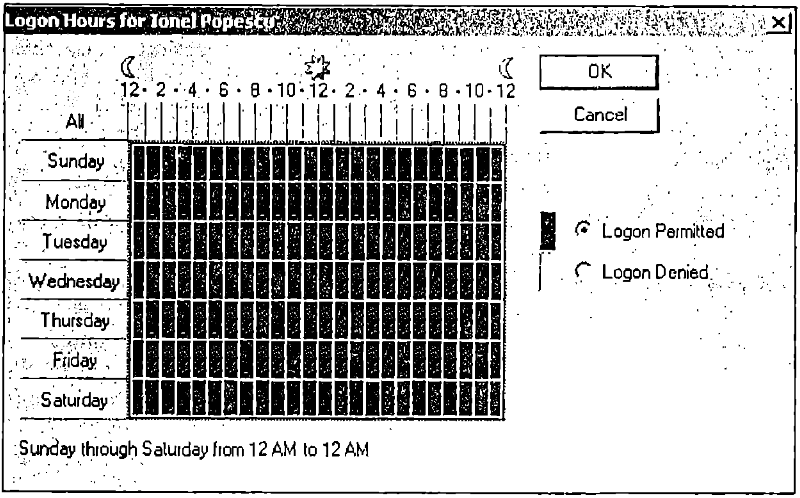


Figura 13.6.4. Fereastra de stabilire a intervalului orar de acces în reţea

Implicit, fiecare utilizator se poate conecta la orice oră din zi sau din noapte la resursele rețelei. Se poate configura însă posibilitatea de acces numai la anumite intervale orare, de exemplu, utilizatorul se poate conecta la rețea numai în ziua de marți de la orele 9 la 15 : selectați tot intervalul orar : Click pe *All* → *Logon Denied* → selectați de la ora 9AM la 3PM în dreptul zilei de marți (Tuesday) → *Logon Permitted* → *OK*.

Un exemplu destul de interesant pe care dorim să-l prezentăm este acela al studenților din cadrul unei instituții. Implicit, aceştia au dreptul să utilizeze toate calculatoarele din toate laboratoarele la orice oră cînd este program sau nu sînt ore. Din păcate, există şi persoane care din rea-voință sau din necunoştință de cauză în acest timp liber încalcă eventualele regulamente în vigoare. Blocarea contului de acces în rețea ar trebui să fie prima acțiune în astfel de cazuri, dar studentul are dreptul de a utiliza calculatorul în cadrul orelor de laborator, pentru că poate chiar plăteşte pentru acest lucru. În acest caz, am fost puşi în situația de a implementa la scară destul de mare acest sistem de alocare a spațiului de lucru pe intervale orare.

Alt exemplu aplicabil în această situație este cel al unei biblioteci în care fiecărui utilizator îi sînt alocate un anumit număr de ore pe zi, între anumite intervale orare.

O altă secțiune din proprietățile contului de utilizator este reprezentată de stațiile de lucru pe care se poate conecta utilizatorul : *Log On To*. Implicit, fiecare utilizator se poate conecta pe orice stație din domeniu (*All computers*) sau se pot configura anumite stații pe care se pot conecta utilizatorii.

- **Profile** - conține informații despre profilul utilizatorului.

Profilul de utilizator conține setările personale ale acestuia la nivel de interfață. În mod clasic, profilul utilizatorului conține următoarele informații grupate pe directoarele Desktop, Favorites, My Documents, Recent, Send To, Start Menu, Templates. Profilul fiecărui utilizator se găseşte în directorul Documents and Settings de pe discul pe care a fost instalat sistemul de operare. Pe lîngă aceste directoare, profilul conține fişierele ntuser.dat şi ntuser.dat.log. Un profil de utilizator poate fi de tip *roaming* sau de tip *mandatory*. Profilul de tip roaming are drept caracteristică faptul că se salvează pe server şi orice modificare a acestuia pe oricare stație de lucru se va reflecta la conectarea pe oricare altă stație de lucru. Profilul mandatory (obligatoriu) se creează pe server şi se pune la dispoziție în rețea prin sharing, mai mulți utilizatori putînd partaja profilul respectiv. Caracteristica profilului obligatoriu este aceea că acest profil nu poate fi modificat, eventualele modificări nefiind salvate pe server.

Crearea unui profil se realizează automat la conectarea pe o stație de lucru. Copierea acestuia într-un profil de tip template se realizează parcurgînd următoarele etape :

- Creați un director pe server pentru profilul utilizatorului (Exemplu, ProfilTmp).
- Puneți-l la dispoziție în rețea şi dați drept de acces grupului Everyone (numele de share, în exemplul nostru, este *profiltmp$* adică este un share de tip administrativ).
- Creați un utilizator obişnuit (de exemplu, nume utilizator : profiltmp).
- La proprietățile utilizatorului nou creat în secțiunea *Profile* la căsuța *Profile path* treceți adresa de acces prin rețea la share-ul respectiv : de exemplu, \\server-01\profiltmp$.
- La *Connect* alegeți din listă o literă disponibilă, iar la *To* aceeaşi adresă ca la pasul anterior ;
- După ce apăsați butonul *OK* sau *Apply* o să vi se afişeze fereastra de mesaje din figura 13.6.5

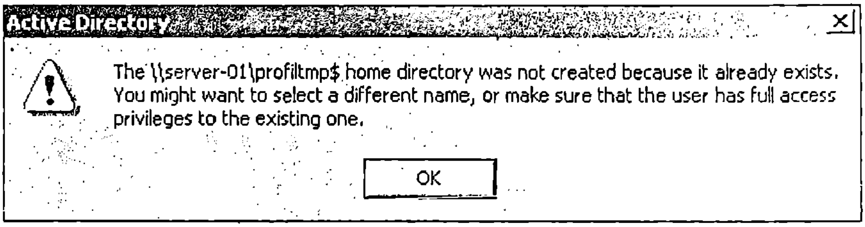


Figura 13.6.5. Mesaj de atenţionare

care ne atenţionează că nu s-a creat directorul pentru stocarea profilului pentru că acesta deja există. Ni se sugerează, de asemenea, să alegem un alt nume de share pentru directorul profilului, dar din experienţa noastră vă informăm că aceasta este calea funcţională a lucrurilor.

- Conectaţi-vă la o staţie de lucru cu utilizatorul nou creat. Vă recomandăm ca staţia de lucru să fie proaspăt instalată.
- Se realizează configurările la nivel de interfaţă, dar şi pentru anumite aplicaţii, cu precădere pentru aplicaţiile de tip Office şi pentru Internet: modul de aşezare a toolbar-urilor, unităţile de măsură, modul de vizualizare a unei pagini, locul în care se salvează implicit documentele, contul de e-mail, paginile favorite, iconiţele de pe desktop etc.
- După delogarea de pe staţia de lucru, pe server în directorul alocat utilizatorului ProfilTmp vor apărea o serie de fişiere şi directoare prezentate în figura 13.6.6.

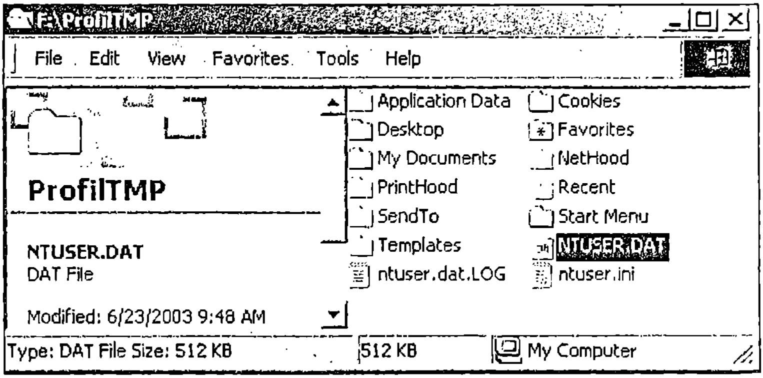


Figura 13.6.6. Conţinutul unui profil de utilizator

- Conectarea pe oricare altă staţie de lucru din domeniu aduce cu sine încărcarea profilului de utilizator direct de pe server, păstrînd toate setările făcute în timpul sesiunilor de lucru. Singurele informaţii care nu se transportă o dată cu profilul utilizatorului sînt fişierele temporare.
- Vizualizarea profilurilor de utilizator înregistrate pe o staţie de lucru se realizează parcurgînd următoarele etape: Rclick (pe My Computer, de pe Desktop sau din meniul Start) → **Properties** → **Advanced** → **Settings** (de la User Profiles).

- Copierea unui profil se realizează prin acționarea butonului *Copy To*, se stabilește calea de salvare prin acționarea butonului **Browse** și se atribuie drept de utilizare grupului de lucru *Everyone* prin acționarea butonului **Change**.

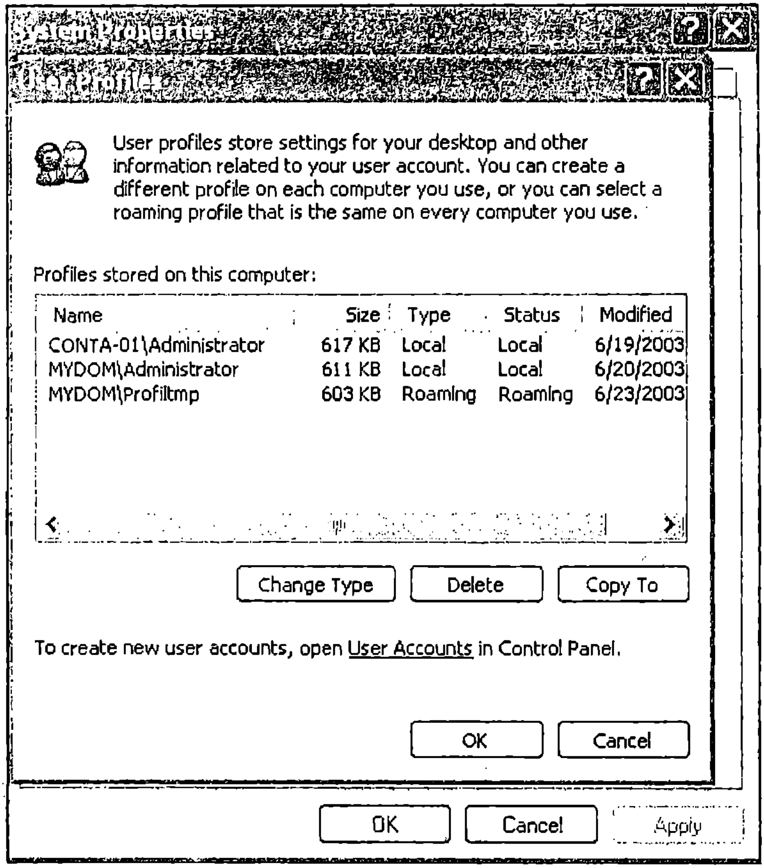


Figura 13.6.7. Profilele de utilizator de pe o stație de lucru

- Schimbarea tipului unui profil se poate realiza numai în cazul profilurilor de tip *Roaming*, prin acționarea butonului *Change Type*.
- Schimbarea profilului de tip *Roaming* în profil obligatoriu (*Mandatory*) se realizează prin schimbarea extensiei fișierului *NTUSER.DAT* în *NTUSER.MAN*, din profilul utilizatorului de pe server.
- În cazul în care profilul de pe server nu este disponibil, se va crea un profil local utilizatorului.

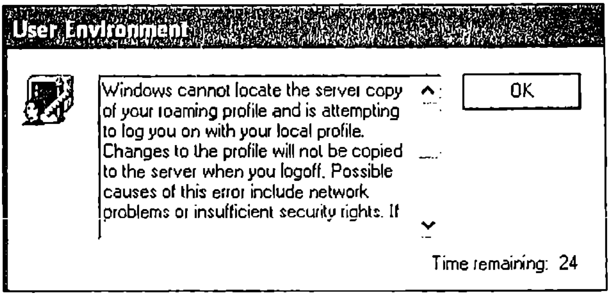


Figura 13.6.8. Mesaj de eroare

Este foarte important ca un profil să fie cît mai mic pentru a fi transportat rapid prin reţea. De aceea încercaţi să eliminaţi cît mai multe informaţii din profilul obligatoriu pe care-l creaţi. Pentru a pune acelaşi profil la dispoziţia mai multor utilizatori, vă recomandăm să copiaţi conţinutul directorului în care a fost creat profilul template într-un alt director, de exemplu *Profile*, pe care puneţi-l la dispoziţie în reţea cu dreptul de citire pentru grupul *Everyone*.

Revenind la fereastra de proprietăţi a utilizatorului, la **Profile**:

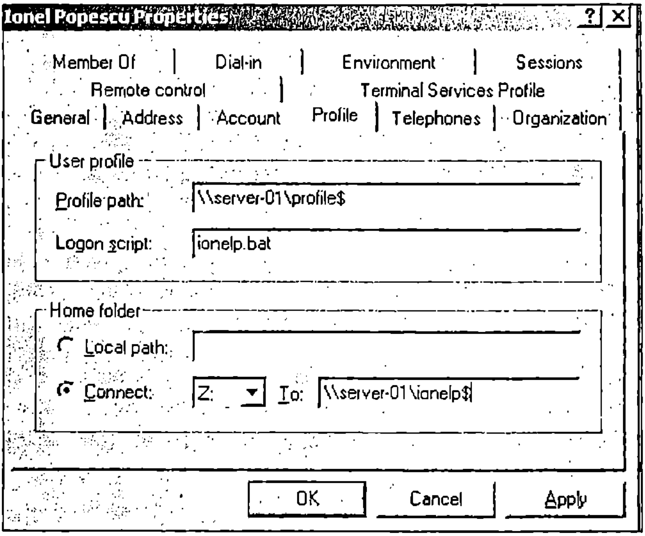


Figura 13.6.9. Stabilirea configuraţiilor pentru profilul unui utilizator

La **Profile path** trecem calea de acces prin reţea la profilul utilizatorului. Dacă este un profil obligatoriu (*Mandatory*), se trece aceeaşi cale pentru mai mulţi utilizatori. În cazul profilurilor *Roaming*, trebuie creat pentru fiecare utilizator un director pe server şi pus la dispoziţie în reţea cu drepturi de acces numai pentru acesta.

Logon Script reprezintă nume unui eventual script care se execută în momentul în care s-a conectat utilizatorul respectiv. Aceste script-uri se execută anterior script-urilor specificate prin politica de securitate (vezi începutul capitolului). Script-urile din această categorie sînt salvate în directorul **C:\WINNT\SYSVOL\sysvol\mydom.myorg.ro\ scripts** și sînt puse la dispoziție în rețea sub denumirea NETLOGON, putînd fi accesate la adresa: \\server-01\NETLOGON. Implicit, în acest director nu se află nici un fișier.

Connect ... To se folosește pentru conectarea utilizatorului, în mod automat, la o resursă de pe server.

Celelalte proprietăți configurabile utilizatorilor sînt:

- **Telephones** - pentru configurarea diferitelor numere de telefoane la care poate fi contactat utilizatorul respectiv.
- **Organization** - diferite date despre poziția în cadrul organizației.
- **Remote Control** - modul de acceptare a accesului la distanță și de interacțiune cu utilizatorul.
- **Terminal Services Profile** - profil de acces pe server folosind Terminal Services.
- **Member Of** - cărui grup de utilizatori aparține utilizatorul curent.
- **Dial-in** - personalizarea accesului în rețea prin dial-up.
- **Environment** - specificarea aplicațiilor care vor fi startate după conectarea la server prin terminal Services.
- **Sessions** - personalizarea modului de sfîrșit al unei sesiuni de lucru.

În momentul creării contului de utilizator, acesta va fi stocat, în mod implicit, în categoria *Users* din Active Directory Users and Computers. Mutarea utilizatorului într-un grup organizațional se realizează cu: RClick (pe utilizator) → **Move** → se alege grupul organizațional din listă → **OK**. În momentul mutării utilizatorului, acesta va prelua toate configurările efectuate în politica de securitate a grupului respectiv.

Pentru o aplicare mai strictă a politicii de securitate pentru un domeniu de calculatoare, vă recomandăm să adăugați și stațiile de lucru în grupul organizațional dorit prin mutarea din categoria *Computers*. După adăugarea la grupul organizațional, stațiile de lucru trebuie repornite pentru aplicarea politicii.

Etapa esențială pentru aplicarea politicii de securitate pe o stație din domeniu este lucrul cu grupuri de utilizatori și adăugarea la acestea a utilizatorilor. Politica de securitate se aplică asupra utilizatorilor prin aceaste grupuri de utilizatori.

Crearea unui grup:

1. RClick pe grupul organizațional dorit → **New** → **Group**.
2. Scrieți numele grupului la **Group Name** → **OK**.

Adăugarea unui utilizator într-un grup de utilizatori:

1. Dublu-click pe grupul de utilizatori creat → **Members**.
2. **Add**, dublu-click pe numele utilizatorului dorit din listă sau scrieți de la tastatură numele utilizatorului → **OK** → **OK**.

Cîteva elemente de administrare

A. Regăsirea utilizatorilor în Active Directory

În A.D.U.C., RClick (pe numele domeniului) → **Find** → la *Name* se specifică numele utilizatorilui → **Find Now**.

Dacă nu cunoaşteţi numele utilizatorului sau doriţi o căutare avansată, apăsaţi pe Advanced, putînd realiza căutări după diferite caracteristici ale utilizatorilor (Butonul Field, opţiunea Users), ale grupurilor sau ale persoanele de contact. La condiţii se pot specifica diferite criterii de căutare:

- care să înceapă cu (*Start with*);
- care să se termine cu (*Ends with*);
- este (*Is exactly*);
- nu este (*Is Not*);
- care conţine (*Present*);
- care nu conţine (*Not Present*).

> Contactele reprezintă informaţii despre diferite persoane gestionate în A.D., dar care nu au drept de conectare în reţeaua curentă.

B. Blocarea/Deblocarea unui cont de utilizator

Blocarea: RClick (pe numele utilizatorului) → **Disable Account**.
Deblocarea: RClick (pe numele utilizatorului) → **Enable Account**.

C. Active Directory Schema

Reprezintă un set de opţiuni extinse de administrare a unui domeniu Windows 2000. Pentru a putea extinde schema Active Directory, trebuie să instalaţi în prealabil toate instrumentele de administrare ale Windows 2000 Server:

1. **Start** → **Settings** → **Control Panel**.
2. Dublu-click **Add/Remove Programs**.
3. Selectaţi **Windows 2000 Administration Tools** → **Change** → **Next**.
4. **Install All Administrative Tools** → **Next**.
5. După ce se termină de copiat şi instalat fişierele, **Finish** → **Close**.

Adăugarea Active Directory Schema într-o consolă de administrare:

1. **Start** → **Run** → scrieţi *MMC* în căsuţa **Open** → **OK**.
2. În meniul **Console** → **Add/Remove Snap-in** → **Add** → **Active Directory Schema** → **Add** → **Close** → **OK**.
3. Consola administrativă poate fi salvată cu un anumit nume: în meniul **Console** → **Save As**, scrieţi numele pe care doriţi să-l daţi consolei (de exemplu, Schema) → **Save**.

Un exemplu clasic de utilizare a schemei Active Directory este aceea a adăugării unei noi proprietăţi utilizatorilor din domeniu, gen nivelul salariului, codul numeric personal etc.

Crearea utilizatorilor folosind comenzi

Comanda de creare a unui utilizator este : **NET USER** care are următoarea sintaxă :

```
net user [username [password | *] [options]] [/domain]
         username {password | *} /add [options] [/domain]
         username [/delete] [/domain]
```

în care :

- *username* reprezintă numele de utilizator. Pentru numele de utilizator cu spații acesta se va trece între ghilimele ;
- *password* reprezintă parola de acces în rețea. Caracterul asterix (*) se folosește pentru a întrerupe execuția comenzii NET cu scopul introducerii parolei de utilizator ;
- */domain* reprezintă numele domeniului în care va fi adăugat utilizatorul respectiv. Dacă contul de utilizator se creează pe serverul de domeniu, această opțiune nu mai este necesară ;
- */add* – parametrul care specifică faptul că utilizatorul este nou ;
- */delete* – se specifică o acțiune de ștergere a utilizatorului ;
- opțiunile principale întîlnite la crearea unui cont sînt :
  - o */active* : {yes|no} – implicit valoarea este Yes ;
  - o */comment* : „text" – specificarea unui comentariu pentru utilizator. Acest text apare la Description din proprietățile generale ale utilizatorului din A.D.
  - o */expires* : {date|never} – data de expirare a contului de utilizator sau specificarea faptului că acesta nu va expira niciodată ;
  - o */fullname* : „name" – specificarea numelui complet al utilizatorului ;
  - o */homedir* : pathname – specificarea directorului la care se conectează automat utilizatorul. Este echivalentul lui Connect...To... de la proprietățile utilizatorului din Active Directory. Acest director trebuie să existe și să fie pus la dispoziție în rețea ! ;
  - o */passwordchg* : {yes|no} – specifică posibilitatea de schimbare a parolei. Implicit este Yes ;
  - o */profilepath* [: path] – specificarea căii de acces la profilul utilizatorului. Acest director trebuie să existe și să fie pus la dispoziție în rețea ;
  - o */scriptpath* : pathname – calea către script-urile de logon sau mai bine spus, numele scriptului respectiv ;
  - o */usercomment* : „text" – alte comentarii care pot fi specificate pentru utilizatorul respectiv.

Exemplu – Crearea unui utilizator cu numele DimaR.

Date preliminare :

Nume server : server-01
Grup utilizatori : Vizitatori
Adresa profilului template : \\server-01\profile$

1. Deschideți utilitarul Command Prompt : **Start** → **Run** → scrieți *cmd* → **OK** ;

2. Poziționarea pe discul pe care vor fi stocate informațiile utilizatorului :

```
F: ↵
```

3. Crearea unui nou director cu numele utilizatorului:

```
MD DimaR
```

4. Punerea la dispoziţie în reţea a informaţiilor din directorul respectiv:

```
net share DimaR$=F:\DimaR
```

5. Crearea utilizatorului:

```
net user DimaR parola /fullname:"Dima Raluca"
/homedir: \\server-01\DimaR$ /profilepath:\\server-01\
profile$ /scriptpath:default.bat /add
```

6. Adăugarea utilizatorului într-un grup de lucru existent:

```
net group vizitatori /add dimar
```

7. Stabilirea setărilor de securitate pentru directorul aferent utilizatorului DimaR:

```
cacls dimar /p Administrator:F DimaR:F /R Everyone /e
```

Existenţa posibilităţii de creare a utilizatorilor folosind script-uri are un rol foarte important în procesul de automatizare a activităţilor, mai ales cînd există informaţii stocate în diferite tipuri de baze de date.

De exemplu, în Visual Fox, operaţiunea de automatizare a creării utilizatorilor constă în crearea unui set de variabile compuse (echivalente fiecărei linii de execuţie) din şiruri de caractere (aferente comenzilor şi parametrilor) şi cîmpuri din baze de date, aferente datelor despre utilizatori, precum şi configurările necesare de genul *nume de servere, domenii* etc. Informaţiile se folosesc pentru inserarea într-o tabelă cu o singură coloană, fiecărei comenzi corespunzîndu-i cîte o linie. Informaţiile din tabela cu comenzi vor fi transferate într-un fişier de tip BAT cu ajutorul secvenţei program:

```
COPY TO numefisier TYPE SDF
RENAME numefisier.TXT TO numefisier.BAT
```

Metode avansate de creare a utilizatorilor

Tehnologiile

O altă metodă de creare a utilizatorilor este aceea a folosirii tehnologiilor de tip LDAP, WMI şi WHS, care permit un control mai amănunţit al informaţiilor despre utilizatorul respectiv, precum şi al politicilor de management în cadrul organizaţiei.

LDAP (*Lightweight Directory Access Protocol*) reprezintă un protocol software care permite oricui să extragă informaţii sau să acceseze alte resurse precum fişiere sau dispozitive din reţea de pe Internet sau din Intranet. Reprezintă o primă versiune a protocolului *Directory Access Protocol* (DAP) şi este considerat *light* (subţire) pentru că nu include opţiunile de securitate. A fost dezvoltat la Universitatea din Michigan şi a fost adoptat de aproximativ 40 de companii, cele mai reprezentative fiind Microsoft, Novell şi CISCO.

LDAP permite regăsirea informaţiilor într-o reţea fără a cunoaşte locaţia exactă a informaţiei respective.

LDAP este organizat într-o structură arborescentă compusă din următoarele niveluri:

- directorul rădăcină (*root directory*), locul din care porneşte căutarea;
- ţara sau, mai bine spus, domeniul din structura DNS (COM, RO, FR);

- organizația - numele organizației ;
- grupul organizațional - subdiviziune logică a organizației care poate fi structurat în : divizii, departamente, filiale ;
- obiecte - include obiectele întîlnite într-un grup organizațional : utilizatori, stații de lucru, fișiere, resurse puse la dispoziție în rețea (share-uri), imprimante.

Windows® Management Instrumentation (*WMI*) este o componentă a sistemului de operare Windows care permite gestionarea informațiilor și controlul rețelelor Windows. Oferă suport pentru medii de dezvoltare a aplicațiilor cum ar fi C++, permițînd conectarea către baze de date folosind ADO sau ODBC. De asemenea, poate fi folosit în automatizarea anumitor activități de rețea prin crearea de script-uri de administrare. Se integrează cu Active Directory și alte soluții oferite de Microsoft : servere de e-mail, de Intenet, de aplicații etc.

Componentele WMI sînt :

- sistemul de notificare a evenimentelor ;
- limbajul de interogare a evenimentelor ;
- suportul pentru securitate ;
- suportul pentru autentificare și conectare la distanță.

Common Information Model (*CIM*) reprezintă un model de date extensibil orientat obiect care conține informații despre diferitele părți ale unei organizații. Împreună cu WMI, un programator poate crea clase care să reprezinte hard discuri, aplicații, routere sau alte tehnologii definite de către acesta.

Script-urile sînt folosite pentru a accesa toate clasele WMI aferente obiectelor hardware sau software din cadrul unei organizații. Script-urile de tip *Windows Script Host* (*WSH*) pot fi folosite pentru a accesa obiecte de tipul fișierelor de sistem, pentru a gestiona imprimante de rețea, pentru schimbarea variabilelor sistem. Scripturile de tip *Active Directory™ Service Interface* (*ADSI*) permit accesul către obiectele din Active Directory folosind un limbaj derivat din *XML* (*eXtended Markup Language*). Împreună, cele două limbaje, WSH și ADSI, permit accesul către obiecte și operațiuni de gestionare a acestora care nu se pot realiza prin scripturile de tip *batch* (BAT - vechiurile script-uri de tip MS-DOS).

Cu aceste limbaje se pot crea rapid aplicații simple sau complexe de management al unei rețele Windows, iar implementat în C++ poate fi folosit pentru controlul tuturor obiectelor dintr-o organizație.

Crearea conturilor de utilizatori folosind WSH

Cu toate că aceste script-uri poartă denumirea de WSH, ele folosesc limbajul VBS (*Visual Basic Script*). Alte variații ale acestui limbaj sînt fișierele de tip WSF (*Windows Script File*), dar a căror sintaxă este diferită.

Crearea unui script :

1. **Start → Programs → Accessories → Notepad.**
2. Scrieți textul script-ului.
3. **File → Save →** la **Save in** alegeți calea de salvare a documentului. (Vă recomandăm ca scripturile de administrare să le gestionați centralizat, într-un director care să nu fie pus la dispoziție în rețea, cel puțin în faza de construcție).
4. La **File name** scrieți numele script-ului, urmat de extensia **VBS → Save.**

Execuţia unui script se realizează, în mod normal, prin dublu-click pe numele fişierului sau din Command Prompt folosind comenzile *cscript* sau *wscript* urmate de numele fişierului şi extensia acestuia. Pentru depanare se pot folosi ferestre de mesaje pentru afişarea valorii diferitelor variabile pe parcursul execuţiei.

Majoritatea erorilor (fig. 13.6.10) oferă informaţii despre linia la care s-a produs eroarea respectivă şi mesajul de eroare. În Notepad, regăsirea erorilor după această metodă este o aventură în cazul script-urilor de dimensiuni foarte mari, pentru că trebuie numărată fiecare linie. Noi folosim în acest scop liniile albe şi introducem comentarii cu numărul liniei curente (vezi listing-ul nr. 13.6.1).

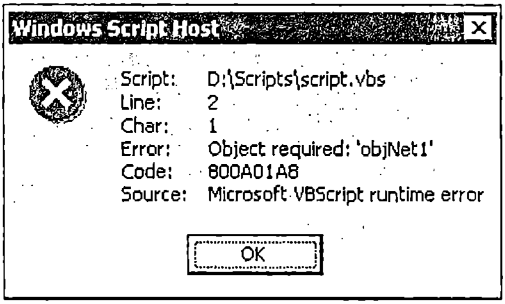


Figura 13.6.10. Fereastră de eroare în execuţia unui script VBS

Listing-ul 13.6.1. Script-ul de creare a unui utilizator într-un domeniu Windows

```
'* La DC se specifică numele întreg al domeniului. Pentru
'* fiecare componentă a acestuia se scrie un nou DC. În
'* cazul nostru, numele complet al domeniului este:
'* mydom.myorg.ro.

'* Conectarea la Domeniu
Set objDomain = GetObject ("LDAP://dc=MYDOM,dc=MYORG,dc=RO")
'* Linia 7
'* Crearea grupului organizaţional
Set objOU = objDomain.Create ("organizationalUnit", "ou=Grup
Nou")
objOU.SetInfo

'* Conectarea la grupul organizaţional
Set objOU = GetObject ("LDAP://OU=GrupNou, dc=MYDOM, dc=
MYORG,DC=RO")

'* Creare utilizatorului cu numele PopescuVasile
Set objUser = objOU.Create ("User", "cn= PopescuVasile")

'* Stabilirea numelui de acces în reţea
objUser.Put "userPrincipalName", "PopescuVasile"
```

```
'* Adăugarea informaţiilor suplimentare pentru contul
'* PopescuVasile.

'* Specificarea numelui aferent domeniilor pre-Windows
'* 2000; în pre- W2k, numele utilizatorilor nu trebuie să
'* fie mai mari de 12 caractere.
'* De asemenea, pot apărea probleme şi la staţiile superioare
'* W2k, de exemplu, XP, cînd numele de utilizator trebuie
'* să fie specificat tot din 12 caractere sau trebuie să
'* fie scris în formatul unei adrese de e-mail: Ex:
'* PopescuVasile@mydom.myorg.ro
objUser.Put "sAMAccountName", "PopescuVasil"

'* Prenumele, iniţiala, numele de familie, numele complet
objUser.Put "givenName", "Vasile"
objUser.Put "initials", "I."
objUser.Put "sn", "Popescu"
objUser.Put "displayName", "Popescu I. Vasile"

'* Adăugarea informaţiilor de localizare a utilizatorului
'* în firmă
objUser.Put "physicalDeliveryOfficeName", "Sala 327a"
objUser.Put "telephoneNumber", " (0232) 20-1418"
objUser.Put "mail", "popescuvasile@myorg.ro"
objUser.Put "wWWHomePage", "http://www.myorg.ro"

'* Crearea directorului pe server pentru utilizator
Set objFSO = CreateObject ("Scripting.FileSystemObject")
Set objFolder = objFSO.CreateFolder ("F:\PopescuVasile")

'* Punerea la dispoziţie în reţea a directorului nou creat
Const FILE_SHARE = 0
Const MAXIMUM_CONNECTIONS = 25
strComputer = "."
Set objWMIService = GetObject ("winmgmts:" &_
"{impersonationLevel=impersonate}!\\" & strComputer & "\root\
cimv2")
Set objNewShare = objWMIService.Get ("Win32_Share")
errReturn = objNewShare.Create _
("F:\PopescuVasile", "PopescuVasile$", FILE_SHARE, _
MAXIMUM_CONNECTIONS, "Directorul lui Vasile de pe server.")

'* Adăugarea informaţiilor cu privire la profilul
'* utilizatorului
```

```
objUser.Put "profilePath", "\\server-01\Profile$"
objUser.Put "scriptPath", "logon.vbs"
objUser.Put "homeDirectory", "\\server-01\PopescuVasile$"
objUser.Put "homeDrive", "Z:"

'* Adăugarea informaţiilor cu privire la numerele de
'* telefon ale utilizatorului
objUser.Put "homePhone", " (0232) 200100"
objUser.Put "pager", " (0232) 200101"
objUser.Put "mobile", " (0555) 202002"
objUser.Put "facsimileTelephoneNumber", " (0232) 20-1070"
objUser.Put "ipPhone", "1418"
objUser.Put "info", "Va rugam sa nu contactati utilizatorul"&_
"acasa decit pentru urgente. Sunati pe mobil sau trimiteti
un fax."

'* Aplicarea configurărilor
objUser.SetInfo

'* Crearea unui grup de utilizatori
Set objOU = GetObject ("LDAP://OU=GrupNou,dc=MYDOM, dc=MYORG,
dc=RO")
Set objGroup = objOU.Create ("Group", "cn=GrupGRP")
objGroup.Put "sAMAccountName", "GrupGRP"
objGroup.SetInfo

'* Adăugarea utilizatorului în noul grup de utilizatori
objGroup.Add objUser.ADSPath


'* Specificarea faptului că acest cont va fi disponibil în
'* reţea.
'* Implicit conturile create cu WHS sînt disabled, adică nu
'* pot fi folosite.
objUser.AccountDisabled = FALSE

'* Specificarea parolei pentru utilizator pentru că,
'* implicit, acesta a fost creat fără parolă.
objUser.SetPassword "po0614"

'* Aplicarea noilor configurări
objUser.SetInfo
```

Un şi mai mare randament în procesul de creare a utilizatorilor este reprezentat de extragerea informaţiilor din baze de date. În exemplul următor, vă propunem o bază de

date de tip SQL Server la care ne vom conecta folosind tehnologii ADO. Vom folosi doar cîteva informaţii esenţiale despre respectivul utilizator, putînd detalia pe larg adăugînd noi cîmpuri în tabelă. În cazul nostru, serverul de baze de date este instalat pe serverul de domeniu (Server-02, vezi figura 13.1.2), deci va avea IP-ul: 172.172.172.2.

Structura tabelei care conţine informaţii despre utilizatori este prezentată în figura 13.6.11.

tblUsr

Column Name	Datatype	Length	Precision	Scale	Allow Nulls
UserName	varchar	50	0	0	☐
Password	varchar	50	0	0	☐
Nume	varchar	50	0	0	☐
Prenume	varchar	50	0	0	☐
email	varchar	50	0	0	☑
Grup	varchar	50	0	0	☐

Figura 13.6.11. Structura tabelei cu informaţii despre utilizatori

În coloana Grup se specifică numele grupului de utilizatori din care va face parte utilizatorul curent.

Crearea parolei pentru organizaţii cu foarte mulţi utilizatori reprezintă un alt subiect de discuţie. Vă recomandăm să folosiţi algoritmi de creare a acestora, bazîndu-vă pe informaţii mai puţin publice. Un exemplu ar fi o combinaţie de litere şi cifre din numele de familie sau CNP, sau data naşterii.

Listing-ul 2. Crearea grupurilor de utilizatori şi a utilizatorilor în mod automat prin preluarea informaţiilor dintr-o bază de date

```
'* Crearea conexiunii către serverul de baze de date
'* Nu este obligatoriu ca acesta să fie SQL Server
set oConn= WScript.CreateObject ("ADODB.Connection")
    oConn.Open = "Provider=SQLOLEDB.1;Password=******; " &_
      "Persist Security Info=True;User ID=AdminBD; " &_
      "Initial Catalog=bdUsers; " &_
       "Data Source=172.172.172.2;Network Library=dbmssocn"

'* Crearea recordset-ului cu numele grupurilor de utilizatori
set recs = WScript.CreateObject ("ADODB.Recordset")
     recs.ActiveConnection = oConn
     recs.Source = "select distinct rtrim (grup) as grupu
     from tblUsr"
     recs.Open ()

'* Conectarea la grupul organizaţional
Set objOU = GetObject ("LDAP://OU=GrupNou,dc=mydom,dc=myorg,
dc=RO")
```

```
'* Parcurgerea recordset-ului
while not recs.eof

   numegrup = rtrim (recs.Fields.Item ("grupu").Value)

'* Crearea Grupului
   Set objGrup = objOU.Create ("Group", "cn=" & numegrup)
       objGrup.Put "sAMAccountName", "" & numegrup
       objGrup.SetInfo

'* Trecerea la următoarea înregistrare din Recordset
   recs.movenext ()
wend

'* Închiderea recordset-ului în vederea repopulării cu
'* informaţii din baza de date
recs.close ()

'* Repopularea recordset-ului
     recs.Source = "select * from tblUsr"
     recs.Open ()

'* Parcurgerea recordset-ului pentru crearea utilizatorilor
while not recs.eof

'* Crearea variabilelor prin care se preiau informaţiile
'* din recordset
   numeuser = rtrim (recs.Fields.Item ("UserName").Value)
   parola = rtrim (recs.Fields.Item ("Password").Value)
   numegrup = rtrim (recs.Fields.Item ("Grup").Value)
   vpren = rtrim (recs.Fields.Item ("Prenume").Value)
   vNume = rtrim (recs.Fields.Item ("Nume").Value)
   vemail = rtrim (recs.Fields.Item ("email").Value)

'* Crearea utilizatorului aferent liniei curente din recordset
   Set objUser = objOU.Create ("User", "cn=" & numeuser)

'* Stabilirea numelui de acces în reţea
   objUser.Put "userPrincipalName", "" & numeuser
   objUser.Put "sAMAccountName", "" & numeuser

'* Prenumele, iniţiala, numele de familie, numele complet,
'* e-mail
   objUser.Put "givenName", "" & vpren
   objUser.Put "sn", "" & vNume
```

```
    objUser.Put "displayName", "" & vPren & " " & vNume
    objUser.Put "mail", "" & vemail

  '* Aplicarea configurărilor
    objUser.SetInfo

  '* Specificarea faptului că acest cont va fi disponibil în
  '* rețea
    objUser.AccountDisabled = FALSE

  '* Specificarea parolei
    objUser.SetPassword "" & parola

  '* Aplicarea noilor configurări
    objUser.SetInfo

  '*  Conectarea  la  un  grupul  de  utilizatori  specific
  '* utilizatorului curent
    Set objAddGroup = GetObject ("LDAP://cn=" & numegrup & _
              ", OU=GrupNou, dc=mydom,dc=myorg, dc=RO")

  '* Adăugarea utilizatorului la grup
    objAddGroup.Add objUser.ADSPath
    objAddGroup.SetInfo

    recs.movenext ()
  wend

  wscript.quit
```

Script-urile pentru crearea utilizatorilor trebuie executate pe serverul de domeniu și de către un utilizator cu drepturi de Administrator.

13.7. Instalarea și configurarea unui server de Web

Instalarea serviciului de Web pentru un server se poate realiza o dată cu instalarea sistemului de operare sau poate fi instalată ulterior:

1. **Start → Settings → Control Panel**;
2. **Add/Remove Programs → Add/Remove Windows Components → Components**;
3. În fereastra *Windows Components Wizard* → click pe *Internet Information Services (IIS)* → **Details**;
4. Activați *Internet Information Services Snap-In*, pentru a putea gestiona serviciul IIS dintr-o consolă administrativă. În această etapă se activează automat și opțiunea Common files;

5. Activaţi opţiunea *World Wide Web Server*;
6. **OK → Next → Next → Finish → Close.**

După efectuarea acestei operaţiuni veţi găsi în Administrative Tools o nouă categorie: *Internet Services Manager* (fig. 13.7.1) din care puteţi gestiona noul d-voastră server de Web.

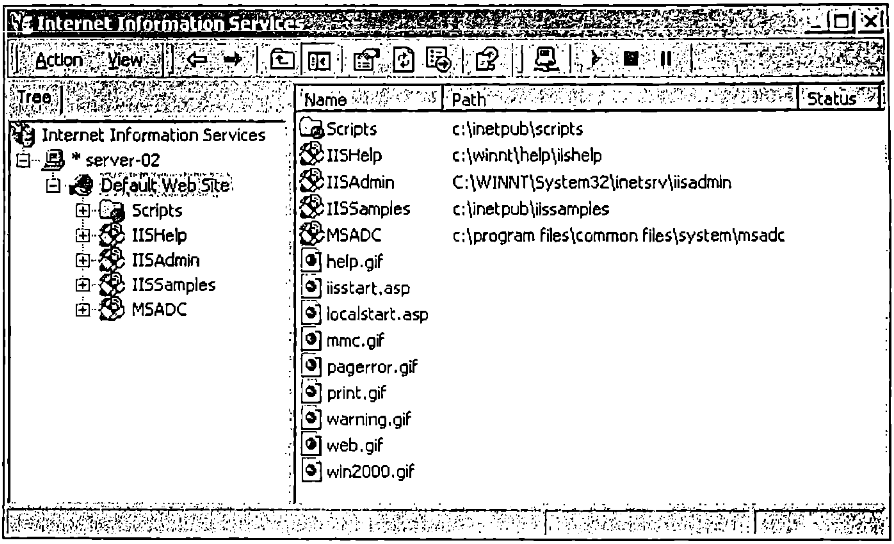


Figura 13.7.1. Internet Service Manager

Pe discul C: de pe sistemul d-voastră veţi descoperi un nou director: *Inetpub*, toate noile pagini pe care le veţi crea fiind găzduite în subdirectorul *wwwroot*.

Verificarea funcţionalităţii serverului se poate face lansînd Internet Explorer, iar la adresă se trece *localhost*. Pagina care se afişează conţine informaţii despre versiunea serverului, documentaţia online, posibilitatea de administrare a serverului.

Pentru crearea propriilor pagini puteţi folosi orice editor de pagini Web sau scrierea codului HTML a paginilor într-un editor de texte. În listing-ul următor vă prezentăm o pagină de start în care va fi specificat faptul că pagina este în construcţie.

Listing-ul 13.7.1. Codul sursă al unei pagini Web

```
<HTML>
<HEAD>
   <TITLE> Bun venit! </TITLE>
</HEAD>

<BODY bgColor="→3A6EA5" text="white">
   <H1><CENTER> Aceasta pagina este inca in constructie! </
```

```
CENTER></H1>
   <P> Va rugam sa reveniti! </P>
</BODY>
</HTML>
```

Culoarea de background specificată la tag-ul <BODY> este echivalentul culorii implicite a background-ului din Windows 2000. Am ales această culoare pentru a putea integra o pagină Web pe desktop-ul stațiilor de lucru din domeniu.

Puteți crea pagina prin introducerea codului direct în *notepad* și salvați cu o anumită denumire (de exemplu, HomePage) și extensia *HTM*, la adresa: C:\Inetpub\wwwroot, vizualizarea acesteia în browser realizîndu-se la adresa http://localhost/HomePage.htm.

Pentru a încărca pagina creată anterior, în mod implicit, cînd se accesează serverul, trebuie să modificați proprietățile implicite ale site-ului d-voastră:

1. În consola de administrare a IIS: RClick pe *Default Web Site* → **Properties**.
2. În fereastra de proprietăți: **Documents** → **Add** → scrieți numele fișierului în căsuța *Default Document Name* (în cazul nostru, HomePage.htm) → **OK**.
3. Poziționați documentul pe primul loc prin apăsarea butonului cu săgeată în sus → **OK**.

În acest moment, pagina d-voastră de start la accesarea serverului, specificînd adresa localhost, va fi cea creată în etapa anterioară.

Adresa la care poate fi accesat serverul Web de pe altă stație de lucru sau oricare alt server din rețea se poate specifica în genul http://nume_calculator/ (în cazul nostru http://WebServer/) sau prin adresa IP (http://194.176.166.101/) (vezi figura 13.1.2).

Instalarea unui server de e-mail într-un domeniu Windows trebuie să se realizeze pe un server declarat mail exchanger în domeniul DNS, care vă oferă acces la Internet. Serverul de e-mail oferit de firma Microsoft este Exchange Server. Acesta se poate integra cu Active Directory și cu SQL Server.

13.8. Configurarea serverului ca un Gateway

Condiția esențială pentru a instala un gateway este existența a cel puțin două interfețe de rețea, una cu conectare directă la Internet (în cazul nostru IP-ul interfeței Internet este: 194.176.165.254, iar pentru interfața internă: 172.172.172.254) și cealaltă destinată rețelei interne.

Atribuirea rolului de router unui server de Windows 2000:

1. **Start** → **Programs** → **Administrative Tools** → **Routing and Remote Access**.
2. RClick pe numele serverului → **Configure and Enable Routing and Remote Access** → **Next**.
3. În fereastra *Common Configurations* (fig. 13.8.1) alegeți opțiunea pe care o doriți (în cazul nostru putem alege ultima variantă, pentru că scopul nostru este de a configura rolul de punte serverului în așa fel încît calculatoarele din rețeaua privată să comunice cu cele din alte rețele) → **Next**.
4. **Finish**.

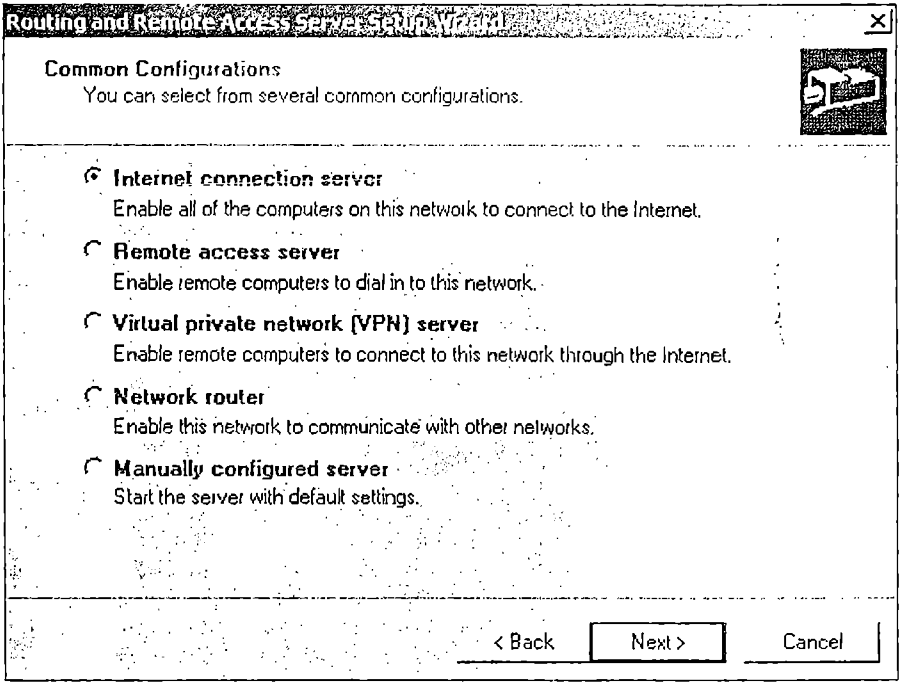


Figura 13.8.1. Alegerea unei configuraţii pentru servere

Un serviciu special care poate fi configurat în această etapă este *NAT* (*Network Address Translation*) care presupune ca staţiile de lucru dintr-un anumit domeniu (Intern) să poată accesa alte reţele de pe Internet prin intermediul interfeţei de reţea reale (cea cu conectare directă la Internet).

Instalarea serviciului NAT:

1. În *Routing and Remote Access*, RClick pe *General* din *IP Routing* → New Routing **Protocol** → *Network Address Translation* (*NAT*) → **OK**.
2. RClick pe *Network Address Translation* (*NAT*) → New Interface.
3. În fereastra *New Interface for...* click pe interfaţa de reţea care face legătură cu reţeaua d-voastră privată → OK.
4. În fereastra *N.A.T. Properties* activaţi opţiunea *Private interface connected to private network* → OK.
5. RClick pe *Network Address Translation* (*NAT*) → New Interface.
6. În fereastra *New Interface for...* click pe interfaţa de reţea care face legătură cu reţeaua Internet → **OK**.
7. În fereastra *N.A.T. Properties* activaţi opţiunea *Public interface connected to the Internet* → *Translate TCP/UDP headers (recommended)* → OK.

După configurarea acestui serviciu, toate staţiile de lucru din domeniul Intern care au trecut de la proprietăţile TCP/IP la secţiunea Gateway, IP-ul intern al serverului, vor putea să acceseze alte reţele de pe Internet.

Pentru controlul accesului, monitorizarea şi controlul traficului precum şi configurarea unui firewall, trebuie instalat pachetul Microsoft Internet Security and Acceleration Server 2000.

13.9. Monitorizarea şi înregistrarea activităţii

Monitorizarea şi înregistrarea activităţii într-o reţea de calculatoare reprezintă una dintre cele mai spinoase probleme în viaţa unei reţele.

Primul pas este acela al înregistrării accesului pe staţii. Vă propunem în acest sens două script-uri: unul de tip batch şi unul de tip *VBS*.

Script-uri de tip batch

Pentru a putea folosi aceste script-uri trebuie să parcurgeţi următoarele etape:

1. Creaţi un director pe unul dintre discurile serverului d-voastră:
   Dublu-click pe iconiţa **My Computer** → dublu-click pe discul pe care doriţi să salvaţi fişierele (de exemplu, Discul C:) → **File** → **New** → **Folder** → tastaţi numele directorului (de exemplu, Loguri) → **Enter**.
2. Puneţi la dispoziţie în reţea acest director prin crearea unui share administrativ şi stabiliţi o politică de securitate pentru share-ul respectiv şi pentru director, în aşa fel încît grupul *Everyone* să aibă dreptul de citire şi scriere în directorul respectiv:
   Varianta a) Rclick pe directorul Loguri → **Sharing** → **Share this folder** → click în căsuţa Share name → adăugaţi la sfîrşitul numelui caracterul dolar ($) → **Permissions** → dezactivaţi opţiunea **Allow** corespondentă categoriei **Full Control** → **OK** → **Security** → dezactivaţi opţiunea **Allow inheritable permissions from parent to propagate to this object** → **Remove** în fereastra *Security* → **Add** → scrieţi *Everyone* sau căutaţi în lista *Name* grupul *Everyone* → **OK** → activaţi opţiunea **Allow** corespondentă categoriei **Write** → **OK**.
   Varianta b) **Start** → **Run** → scrieţi *cmd* în căsuţa **Open** → **OK** → scrieţi CD\ pentru a ajunge în directorul rădăcină şi apăsaţi **Enter** → tastaţi *net share Loguri$=C:\Loguri* pentru crearea share-ului şi apăsaţi **Enter**. Dacă va apărea mesajul *Loguri$ was shared successfully*, scrieţi *exit* şi apăsaţi **Enter**. Pentru crearea unei politici de securitate pentru director se foloseşte comanda *cacls*.

> *Pont*: Pentru afişarea sintaxei unei comenzi în command prompt, scrieţi numele acesteia urmată de caracterele „/?" sau scrieţi „help" urmat de numele comenzii. Comanda NET nu suportă a doua variantă de afişare a sintaxei. De exemplu: *help cacls*, *net share /?*, *cacls /?*.

3. Lansaţi un editor de texte (de exemplu, Notepad):
   Start → **Run** → scrieţi *notepad* în căsuţa **Open** → **OK**.
4. Scrieţi corpul script-ului şi salvaţi în directorul: %windir%\sysvol\ sysvol\ numedomeniudns\ scripts (în cazul nostru: C:\WINNT\ SYSVOL\ sysvol\ mydom.myorg.ro \scripts) specificînd nume diferite pentru script-urile de *logon* şi *logoff*. La salvare, specificaţi extensia *BAT* fişierelor d-voastră.

Pont: %windir% este variabila de sistem prin care majoritatea aplicaţiilor identifică directorul Winnt din Windows 2000 sau directorul Windows din Windows XP. Altă variabilă de sistem pentru a identifica directorul de instalare a sistemului de operare este %System Root%.

5. Adăugaţi script-ul în politica de securitate a utilizatorului:
   Start → **Programs** → **Administrative Tools** → **Active Directory Users and Computers** → RClick pe Grupul organizaţional din care fac parte utilizatorii pentru care se doreşte aplicarea script-urilor (în cazul nostru Vizitatori) → **Properties** → **Group Policy** → **Edit** → navigaţi pînă la adresa *User Configuration\ Windows Settings\ Scripts* → dublu-click pe **Logon** → **Add** → **Browse** → navigaţi de la lista **Look In** pînă la adresa: *C:\WINNT\SYSVOL\sysvol\ mydom.myorg.ro\scripts* → click pe fişierul *Logon* → **Open** → **OK** → **OK** în fereastra *Logon Properties* → dublu click pe **Logoff** → **Add** → **Browse** → navigaţi la adresa specificată mai sus → click pe *Logoff* → **Open** → **OK** → **OK** în fereastra *Logoff Properties* → închideţi ferestrele.

Pont: Pentru afişarea variabilelor de sistem care pot fi folosite în construcţia script-urilor de tip batch se foloseşte comanda SET în command prompt.

Listing-ul 13.9.1. logon.bat

```
echo Logon, %username%, %computername%, %date%, %time% >>
\\server-01\loguri$\loguri.csv
echo Logon, %username%, %computername%, %date%, %time% >>
\\server-02\loguri$\loguri.csv
```

Listing-ul 13.9.2. logoff.bat

```
echo Logoff, %username%, %computername%, %date%, %time% >>
\\server-01\loguri$\loguri.csv
echo Logoff, %username%, %computername%, %date%, %time% >>
\\server-02\loguri$\loguri.csv
```

Explicaţii:

- *echo* este comanda care afişează/scrie anumite mesaje;
- > > *sînt* caracterele care specifică faptul că informaţiile prevăzute de *echo* vor fi adăugate sub forma unei noi linii într-un fişier specificat ulterior (*append*);
- *logon/logoff* reprezintă tipul acţiunii pe care o desfăşoară utilizatorul;
- *%username%* este variabila de sistem care preia numele utilizatorului conectat pe o staţie;
- *%computername%* – numele staţiei de lucru curente, cea pe care se execută script-ul;
- *%date%* şi *%time%* reprezintă data şi ora sistemului pe care se realizează conectarea.

Fişierul *loguri.csv* nu trebuie să existe în momentul creării pe server. Acesta se creează la prima conectare a unui utilizator pe o staţie de lucru şi creşte în dimensiune pe parcursul utilizării reţelei. Analiza datelor din fişierul respectiv se poate realiza cu ajutorul unei aplicaţii care poate interpreta fişiere de tip CSV (*comma separated value*), cea mai cunoscută fiind Microsoft Excel.

Dezavantajul major al utilizării acestor tipuri de script-uri este dat de fapul că în momente de aglomerare a reţelei informaţiile din acest fişier se pot pierde. Aici poate interveni al doilea server (server-02) pe care se pot salva aceleaşi informaţii cu scopul de a asigura o siguranţă sporită a datelor. Chiar şi în acest caz se pot pierde informaţiile din fişiere. Nu vă putem da o explicaţie exactă privitoare la acest fenomen.

Listing-ul 13.9.3. Cîteva înregistrări din conţinutul fişierului loguri.csv

```
Logon, GigelP, Conta-01,Fri 12/06/2003, 19:51:58.34
Logon, IonelP, Conta-02,Fri 12/06/2003, 19:53:04.79
Logoff, GigelP, Conta-01,Fri 12/06/2003, 19:53:23.79
Logon, UserNou, Market-01,Fri 12/06/2003, 19:53:25.75
Logoff, IonelP, Conta-02,Fri 12/06/2003, 19:53:33.44
Logoff, UserNou, Market-01,Fri 12/06/2003, 19:55:49.88
```

Script-uri de tip WHS

O metodă mult mai sigură şi mult mai performantă de înregistrare a accesului în reţea este reprezentată de folosirea script-urilor de tip WHS în corelaţie cu baze de date. Esenţial pentru utilizarea acestor tipuri de script-uri este să aveţi instalat şi configurat un server drept suport pentru baze de date. Dacă serverul d-voastră de domeniu este îndeajuns de puternic, puteţi să-l folosiţi pentru această operaţiune, dar noi recomandăm utilizarea altui server din reţea.

În exemplul următor folosim o bază de date SQL Server instalată pe Server-01 care conţine o tabelă tblLog a cărei structură este prezentată în figura 13.9.1.

tblLog

Column Name	Datatype	Length	Precision	Scale	Allow Nulls	Default Value
DataOra	datetime	8	0	0	☐	(getdate())
TipCon	char	10	0	0	☑	
UserName	char	15	0	0	☑	
statie	char	20	0	0	☑	

Figura 13.9.1. Structura tabelei pentru urmărirea accesului

DataOra este cîmpul care se completează automat în momentul inserării unei noi înregistrări. *TipCon* va conţine informaţii despre tipul conexiunii: Logon sau Logoff.

Pentru a putea folosi aceste script-uri, trebuie să parcurgeţi următoarele etape:

1. Lansaţi un editor de texte (de exemplu, Notepad).

2. Scrieţi corpul script-ului şi salvaţi în directorul: %windir%\sysvol\sysvol\numedomeniudns\scripts (în cazul nostru: C:\WINNT\ SYSVOL\sysvol\mydom.myorg.ro\scripts), specificînd nume diferite pentru scripturile de *logon* şi *logoff*. La salvare specificaţi extensia *VBS* fişierelor d-voastră.
3. Adăugaţi script-ul în politica de securitate a utilizatorului (vedeţi punctul 5 de la metoda anterioară).

Listing-ul 13.9.4. logon.vbs

```
'* Begin of Script
'* Crearea unui obiect de tip reţea care permite accesul la
obiecte '* de genul Username, Computername.
Set objNet = WScript.CreateObject ("WScript.Network")

'* Crearea unui obiect de tip conexiune către serverul de
'* baze de date
set oConn= WScript.CreateObject ("ADODB.Connection")
    oConn.Open = "Provider=SQLOLEDB.1;Password=******; " &_
          "Persist Security Info=True;User ID=AdminBD; " &_
          "Initial Catalog=bdUsers; " &_
          "Data Source=172.17.13.1;Network Library=dbmssocn"

'* Introducerea în baza de date a informaţiilor
sqlIns = "INSERT INTO tblLog (TipCon, UserName, Statie)
VALUES " &_
    " ('Logon', '"& objNet.UserName & "','" & _
    objNet.Computername & "')"
oConn.Execute = sqlIns

'* Ieşirea din script
wscript.quit
'* End of Script
```

Dacă utilizaţi alt suport pentru baze de date, trebuie să schimbaţi linia pentru deschiderea conexiunii către acesta. Dacă utilizaţi baze de date de tip Microsoft Access sau Visual FoxPro, baza de date trebuie să fie salvată în acelaşi loc cu script-urile, ceea ce aduce un spor de nesiguranţă asupra datelor, avînd în vedere faptul că script-urile se află salvate într-o locaţie publică în reţea.

Monitorizarea proceselor lansate de utilizator

Un aspect foarte important în reţelele mari este acela al monitorizării aplicaţiilor care se lansează de fiecare utilizator în parte. Introducerea unui script de logon asemănător celui din listing-ul 13.9.5 vă poate creşte nivelul calitativ al utilizării reţelei din prisma utilizatorilor.

Listing-ul 13.9.5. Procesul de monitorizare şi înregistrare a aplicaţiilor lansate pe o staţie de lucru

```
'* Begin of Script
'* Crearea unui obiect de tip reţea care permite accesul la
'* obiecte de genul  Username, Computername.
Set objNet = WScript.CreateObject ("WScript.Network")

'* Lansarea unui mesaj care-l atenţionează despre faptul că
'* activitatea sa este monitorizată în scopul conştientizării
'* acestuia asupra operaţiilor pe care le va efectua pe
'* staţia de lucru
msgbox ("Salut " & objNet.Username & _
   "! Activitatea pe aceasta statie de lucru este
monitorizata!")

'* Crearea unui obiect de tip conexiune către serverul de
'* baze de date
set oConn= WScript.CreateObject ("ADODB.Connection")
    oConn.Open =  "Provider=SQLOLEDB.1;Password=******; " &_
        "Persist Security Info=True;User ID=AdminBD; " &_
        "Initial Catalog=bdUsers; " &_
        "Data Source=172.17.13.1;Network Library=dbmssocn"

'* Conectarea la Windows Management Instrumentation
strComputer = "."
Set objWMIService = GetObject ("winmgmts:" & _
    "{impersonationLevel=impersonate}!\\" & strComputer &_
    "\root\cimv2")

'* Extragerea din WMIService a proceselelor care se vor crea
Set colMonitoredProcesses = objWMIService. _
   ExecNotificationQuery ("select * from __instancecreatione
   vent "&_
   " within 1 where TargetInstance isa 'Win32_Process'")


'* Artificiu de programare care păstrează script-ul activ
'* în memoria sistemului
i = 0
Do While i = 0
   Set objLatestProcess = colMonitoredProcesses.NextEvent

'* Introducerea în baza de date a informaţiilor despre
```

```
'* noile procese deschise de utilizator
     sqlIns = "INSERT INTO tblProcese (UsrName, Statia,
     Proces)" &_
         "VALUES ('"& objNet.UserName & "','" &_
         objNet.Computername & "', '" & _
         objLatestProcess.TargetInstance.Name & "')"
    oConn.Execute = sqlIns

'* Verificarea unui proces. De exemplu, nu dorim ca
'* utilizatorii să execute aplicaţie Solitaire a cărui
'* executabil este sol.exe
   if objLatestProcess.TargetInstance.Name = "sol.exe" Then
     msgbox ("S-a lansat Solitatire-ul pe statia " &_
                objNet.Computername & " de catre userul " &_
                 objNet.UserName)

'* Închiderea procesului prohibit
   Set colProcessList = objWMIService.ExecQuery _
       ("Select * from Win32_Process Where Name = 'sol.exe'")
   For Each objProcess in colProcessList
        objProcess.Terminate ()
   Next
    end if
Loop
'* End of Script
```

Alte exemple de script-uri

Maparea unui disc din reţea şi crearea unui shortcut pe desktop

```
'* Begin of Script
'* Crearea obiectelor de tip network şi de tip shell (modul
'* în care sînt afişate anumite obiecte pe desktop)
Set objNet = WScript.CreateObject ("WScript.Network")
Set WshShell = CreateObject ("WScript.Shell")
DesktopPath = WshShell.SpecialFolders ("Desktop")

'* Maparea automată a directorului Muzica de pe server pus la
'* dispoziţie în reţea în mod administrativ.
objNet.MapNetworkDrive "M:", "\\server-01\muzica$","True"

'* Crearea unei iconiţie pe desktop care face legătură la
'* discul M:
Set link = WshShell.CreateShortcut (DesktopPath & "\Muzica.lnk")
```

```
link.Description = "Muzica de pe server"
link.HotKey = "CTRL+ALT+SHIFT+M"
link.IconLocation = "explorer.exe,0"
link.TargetPath = "m:"
link.WindowStyle = 3
link.Save
'* End of Script
```

Conectarea la o imprimantă din rețea

```
'* Begin of Script
'* Inițializarea obiectelor
Set objNet = WScript.CreateObject ("WScript.Network")
Set WshShell = CreateObject ("WScript.Shell")
DesktopPath = WshShell.SpecialFolders ("Desktop")

'* Calea către imprimantă care este instalată pe server și
'* este pusă
'* la dispoziție în rețea sub denumirea ImprimantaSRV$
PrinterPath = "\\server-01\ImprimantaSRV$"
objNet.AddWindowsPrinterConnection PrinterPath
objNet.SetDefaultPrinter PrinterPath
'* End of Script
```

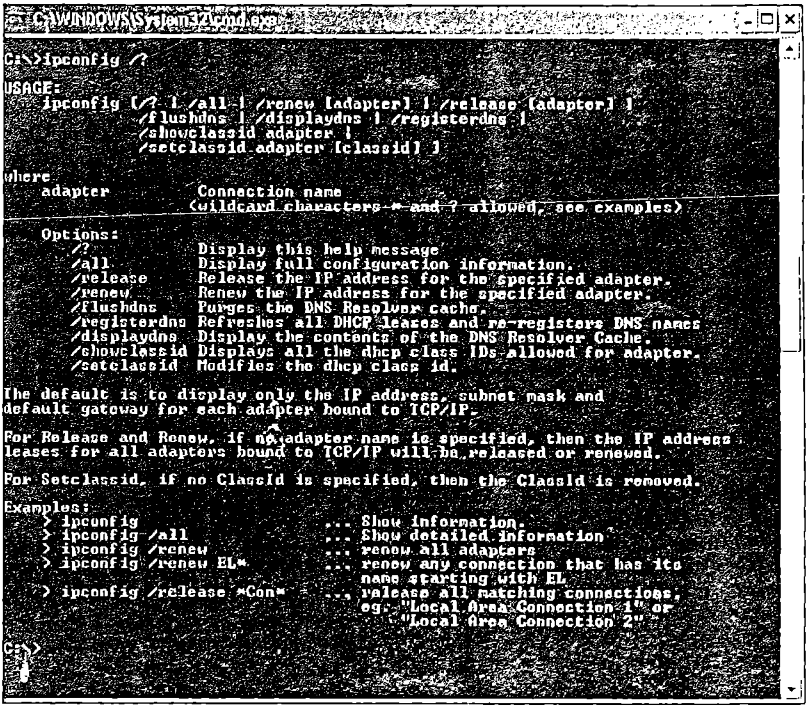
13.10. Instrumente pentru depanare

Windows-ul pune la dispoziția administratorilor o suită de aplicații pentru depanarea rețelei, disponibilă în Resource Kit. Chiar dacă rețeaua a fost proiectată și dată în producție, administratorul va fi nevoit să răspundă în timp la întrebări cum ar fi :

- Ce funcționează bine și ce nu?
- Ce implicații are nefuncționarea rețelei?
- Ce modificări au apărut în rețea?

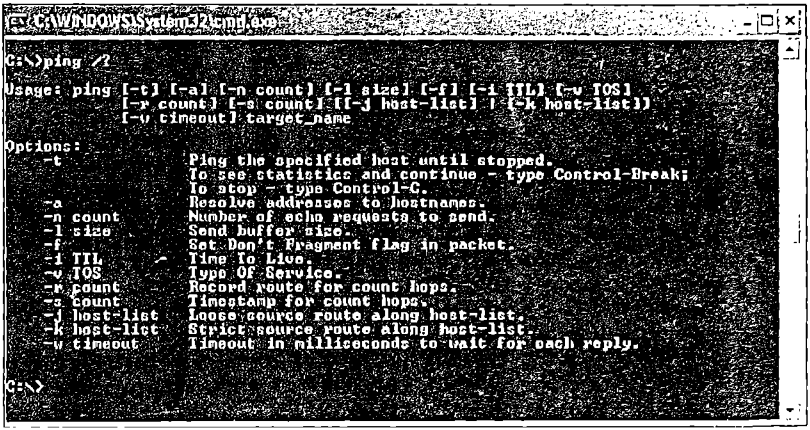
Identificarea și rezolvarea problemelor din rețea trebuie făcută tot structurat. Comenzile prezentate în continuare respectă această cerință.

IPConfig este un utilitar de tip linie de comandă care afișează configurațiile TCP/IP ale unui calculator. Folosirea parametrului /all în sitaxa sa va afișa un raport complet al tuturor interfețelor calculatorului respectiv. Aceste informații pot fi salvate într-un fișier text pentru utilizările ulterioare.



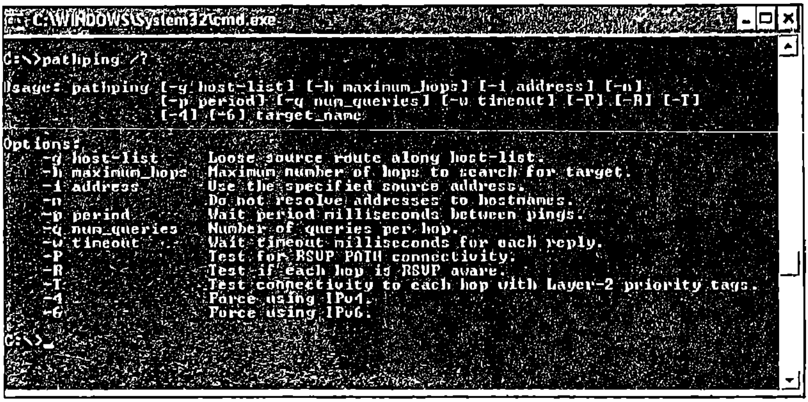
```
C:\WINDOWS\System32\cmd.exe
C:\>ipconfig /?

USAGE:
    ipconfig [/? | /all | /renew [adapter] | /release [adapter] |
              /flushdns | /displaydns | /registerdns |
              /showclassid adapter |
              /setclassid adapter [classid] ]
where
    adapter             Connection name
                       (wildcard characters * and ? allowed, see examples)

    Options:
       /?               Display this help message
       /all             Display full configuration information.
       /release         Release the IP address for the specified adapter.
       /renew           Renew the IP address for the specified adapter.
       /flushdns        Purges the DNS Resolver cache.
       /registerdns     Refreshes all DHCP leases and re-registers DNS names
       /displaydns      Display the contents of the DNS Resolver Cache.
       /showclassid     Displays all the dhcp class IDs allowed for adapter.
       /setclassid      Modifies the dhcp class id.

The default is to display only the IP address, subnet mask and
default gateway for each adapter bound to TCP/IP.

For Release and Renew, if no adapter name is specified, then the IP address
leases for all adapters bound to TCP/IP will be released or renewed.

For Setclassid, if no ClassId is specified, then the ClassId is removed.

Examples:
    > ipconfig                   ... Show information.
    > ipconfig /all              ... Show detailed information
    > ipconfig /renew            ... renew all adapters
    > ipconfig /renew EL*        ... renew any connection that has its
                                     name starting with EL
    > ipconfig /release *Con*    ... release all matching connections,
                                     eg. "Local Area Connection 1" or
                                         "Local Area Connection 2"

C:\>
```

Ping este instrumentul prin care se verifică, în principal, disponibilitatea unui calculator din reţea. Utilitarul trimite o cerere ICMP către adresa IP sau numele calculatorului ţintă. Cel mai simplu test prin care se verifică dacă un calculator din reţea răspunde sau nu presupune „pinguirea" adresei IP a acestuia. Dacă se apelează numele şi acesta nu răspunde, nu înseamnă în mod automat că respectivul calculator are o problemă. Este posibil ca numele să nu poată fi rezolvat de Windows.



```
C:\WINDOWS\System32\cmd.exe
C:\>ping /?

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] target_name

Options:
    -t             Ping the specified host until stopped.
                   To see statistics and continue - type Control-Break;
                   To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        Send buffer size.
    -f             Set Don't Fragment flag in packet.
    -i TTL         Time To Live.
    -v TOS         Type Of Service.
    -r count       Record route for count hops.
    -s count       Timestamp for count hops.
    -j host-list   Loose source route along host-list.
    -k host-list   Strict source route along host-list.
    -w timeout     Timeout in milliseconds to wait for each reply.

C:\>
```

Comanda **Pathping** este un utilitar prin intermediul căruia se transmit pachete către fiecare router din calea către un anumit calculator, pentru a identifica care routere sau legături sînt cu probleme.



```
C:\WINDOWS\System32\cmd.exe

C:\>pathping /?

Usage: pathping [-g host-list] [-h maximum_hops] [-i address] [-n]
                [-p period] [-q num_queries] [-w timeout] [-P] [-R] [-T]
                [-4] [-6] target_name

Options:
    -g host-list     Loose source route along host-list.
    -h maximum_hops  Maximum number of hops to search for target.
    -i address       Use the specified source address.
    -n               Do not resolve addresses to hostnames.
    -p period        Wait period milliseconds between pings.
    -q num_queries   Number of queries per hop.
    -w timeout       Wait timeout milliseconds for each reply.
    -P               Test for RSVP PATH connectivity.
    -R               Test if each hop is RSVP aware.
    -T               Test connectivity to each hop with Layer-2 priority tags.
    -4               Force using IPv4.
    -6               Force using IPv6.

C:\>_
```

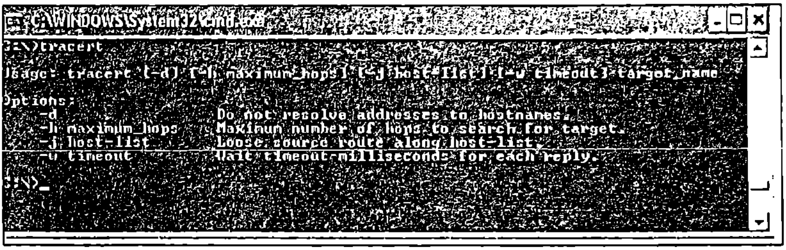
Cînd rulaţi această comandă, veţi observa că prima parte a rezultatului afişat seamănă cu cel al comenzii tracert. După o perioadă de „gîndire", comanda continuă să afişeze informaţiile preluate de la toate routerele din cale. Dintre acestea, cele mai importante sînt cele referitoare la procentul de pachete care se pierd pe o anumită legătură (respectiva legătură este congestionată).

Pentru a vizualiza conţinutul ARP se foloseşte comanda cu acelaşi nume : **arp**. Dacă două calculatoare de pe acelaşi segment nu se văd între ele (nu răspund la ping), se va rula această comandă pe fiecare dintre ele pentru a vedea dacă în tabela ARP există înregistrări referitoare la adresa MAC (**arp -a**).

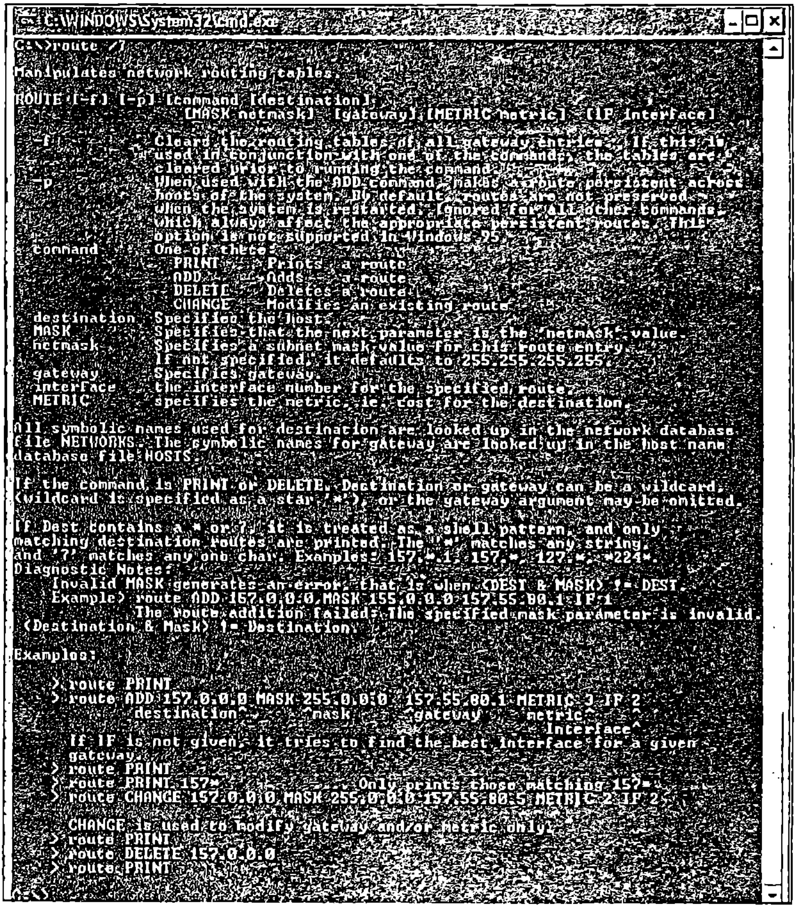
Un alt caz cînd se recomandă folosirea acestei comezi : două calculatoare folosesc aceeaşi adresă IP şi trebuie identificate.

```
C:\WINDOWS\System32\cmd.exe

C:\>arp /?

Displays and modifies the IP-to-Physical address translation tables used by
address resolution protocol (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr]

  -a            Displays current ARP entries by interrogating the current
                protocol data.  If inet_addr is specified, the IP and Physical
                addresses for only the specified computer are displayed.  If
                more than one network interface uses ARP, entries for each ARP
                table are displayed.
  -g            Same as -a.
  inet_addr     Specifies an internet address.
  -N if_addr    Displays the ARP entries for the network interface specified
                by if_addr.
  -d            Deletes the host specified by inet_addr. inet_addr may be
                wildcarded with * to delete all hosts.
  -s            Adds the host and associates the Internet address inet_addr
                with the Physical address eth_addr.  The Physical address is
                given as 6 hexadecimal bytes separated by hyphens. The entry
                is permanent.
  eth_addr      Specifies a physical address.
  if_addr       If present, this specifies the Internet address of the
                interface whose address translation table should be modified.
                If not present, the first applicable interface will be used.
Example:
  > arp -s 157.55.85.212   00-aa-00-62-c6-09  .... Adds a static entry.
  > arp -a                                    .... Displays the arp table.

C:\>
```

Tracert este utilitarul prin care se identifică ruta pe care o traversează pachetele pentru a ajunge la calculatorul destinatar (routerele prin care trec pachetele).



Utilitarul **route** se foloseşte pentru a modifica tabelele de rutare. Se foloseşte mai ales în cazul gateway-urilor, atunci cînd se doreşte ca host-urile dintr-o reţea să poată accesa o alta.



Netstat este comanda prin care se afişează informaţii despre protocoalele care rulează şi conexiunile TCP/IP de pe o staţie. Se recomandă folosirea lui mai ales în situaţiile în care bănuiţi că reţeaua este atacată. Dacă multe din conexiunile afişate sînt în starea SYN, se poate bănui că este vorba despre un atac.

```
C:\WINDOWS\System32\cmd.exe

C:\>netstat /?

Displays protocol statistics and current TCP/IP network connections.

NETSTAT [-a] [-e] [-n] [-o] [-s] [-p proto] [-r] [interval]

  -a            Displays all connections and listening ports.
  -e            Displays Ethernet statistics. This may be combined with the -s
                option.
  -n            Displays addresses and port numbers in numerical form.
  -o            Displays the owning process ID associated with each connection.
  -p proto      Shows connections for the protocol specified by proto; proto
                may be any of: TCP, UDP, TCPv6, or UDPv6.  If used with the -s
                option to display per-protocol statistics, proto may be any of:
                IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6.
  -r            Displays the routing table.
  -s            Displays per-protocol statistics.  By default, statistics are
                shown for IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, and UDPv6;
                the -p option may be used to specify a subset of the default.
  interval      Redisplays selected statistics, pausing interval seconds
                between each display.  Press CTRL+C to stop redisplaying
                statistics.  If omitted, netstat will print the current
                configuration information once.

C:\>
```

Pentru problemele legate de numele NetBIOS se foloseşte utilitarul **nbtstat**. În funcţie de parametrii folosiţi, afişează numele aplicaţiilor, cache-ul NetBIOS etc.

```
C:\WINDOWS\System32\cmd.exe

C:\>nbtstat /?

Displays protocol statistics and current TCP/IP connections using NBT
(NetBIOS over TCP/IP).

NBTSTAT [ [-a RemoteName] [-A IP address] [-c] [-n]
        [-r] [-R] [-RR] [-s] [-S] [interval] ]

  -a   (adapter status) Lists the remote machine's name table given its name
  -A   (Adapter status) Lists the remote machine's name table given its
                        IP address.
  -c   (cache)          Lists NBT's cache of remote [machine] names and their IP
 addresses
  -n   (names)          Lists local NetBIOS names.
  -r   (resolved)       Lists names resolved by broadcast and via WINS
  -R   (Reload)         Purges and reloads the remote cache name table
  -S   (Sessions)       Lists sessions table with the destination IP addresses
  -s   (sessions)       Lists sessions table converting destination IP
                        addresses to computer NETBIOS names.
  -RR  (ReleaseRefresh) Sends Name Release packets to WINS and then, starts Refr
esh

  RemoteName   Remote host machine name.
  IP address   Dotted decimal representation of the IP address.
  interval     Redisplays selected statistics, pausing interval seconds
               between each display. Press Ctrl+C to stop redisplaying
               statistics.

C:\>
```

CAPITOLUL 14

Utilitare de administrare

14.1. Utilitare pentru accesul centralizat la resursele rețelei

Din această categorie amintim utilitarele *Hyena* (SystemTools Software Inc.) și *DameWare NT Utilities* (DameWare Development).

Caracteristica principală a acestor utilitare este de centralizare a acțiunilor de administrare a resurselor unei rețele de calculatoare. Principalele resurse care pot fi gestionate cu ajutorul acestora sînt:

- serverele de domeniu;
- stațiile de lucru cu acces la: discuri, resurse puse la dispoziție în rețea (share-uri), regiștrii sistemului de operare, imprimante, procesele și serviciile active cu posibilitatea opririi sau pornirii acestora, utilizatorii locali, sesiunile deschise, gestiunea resurselor hardware, vizualizarea jurnalelor de activitate (*Event Viewer*). Alte facilități sînt acelea de preluare a controlului, trimiterea de mesaje, crearea de fișiere și directoare de la distanță, copierea de fișiere și directoare (numai în DameWare), închiderea sau repornirea stației de lucru;
- utilizatorii și grupurile din domeniu cu posibilitatea căutării, modificării și ștergerii acestora, precum și a drepturilor pe care le au pe stațiile de lucru din rețea. DameWare aduce ca element în plus în proprietățile utilizatorilor posibilitatea de a introduce o fotografie a acestuia.

Una dintre facilitățile pe care le utilizăm cu preponderență este aceea de vizualizare a sesiunilor de lucru deschise pe servere, precum și a fișierelor accesate.

În plus, DameWare permite preluarea controlului total al unei stații de lucru asemănător serviciului Terminal Service, numai că lucrul pe stația de la distanță se realizează vizibil și interactiv. Această facilitate este inspirată din virusul de tip cal troian NetBus, transformat ulterior într-o aplicație de tip client server, și este foarte utilă în rezolvarea anumitor probleme de la distanță, interacționînd și conlucrînd cu utilizatorul.

O altă facilitate a celor două utilitare este aceea de export al informațiilor din domeniu, în format text sau CSV.

14.2. Utilitare de monitorizare a traficului

Monitorizarea traficului în rețea se poate realiza din Windows cu ajutorul utilitarului Microsoft Network Monitor (fig. 14.2.1) care se poate instala o dată cu sistemul de operare. Informațiile oferite de acesta sînt, în general, de ordin statistic: gradul de utilizare a rețelei, numărul de cadre pe secundă, numărul de biți pe secundă, broadcast-ul și multicast-ul înregistrat în rețea. Altă facilitate este aceea de filtrare a informațiilor și de decodificare a pachetelor în care se dau informații detaliate despre pachete, sursa și destinația acestora, precum și conținutul și dimensiunile lor, cu posibilitatea de salvare a acestor informații.

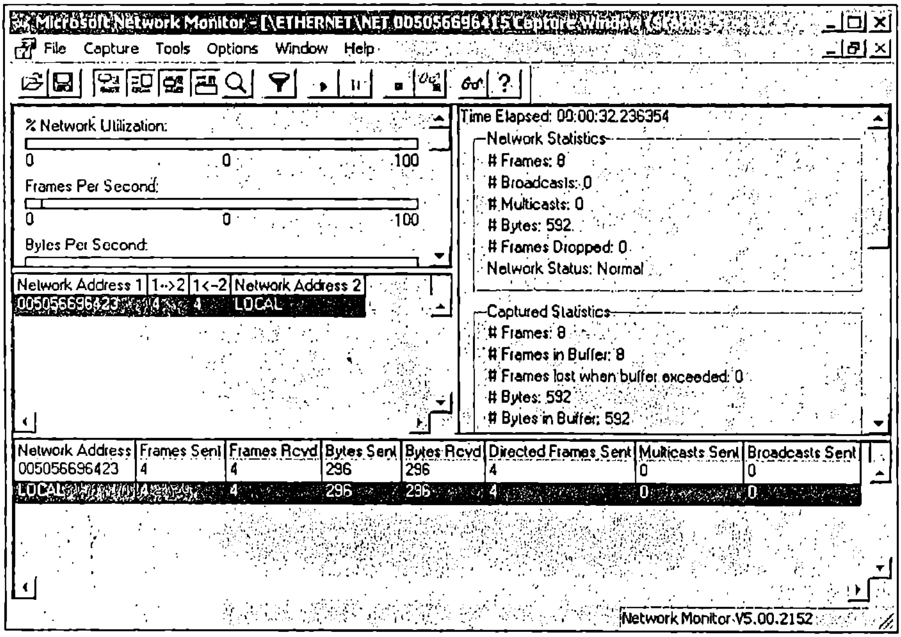


Figura 14.2.1. Utilitarul Network Monitor

Un utilitar mai avansat este IRIS - The Network Traffic Analyzer (eEye Digital Security) (fig. 14.2.2).

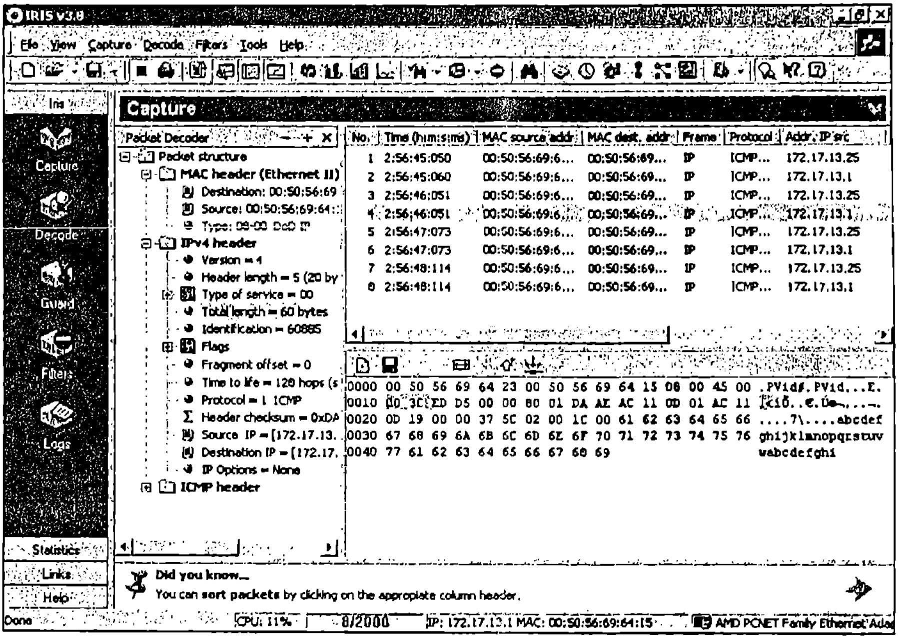


Figura 14.2.2. Utilitarul IRIS

Pe lîngă operaţiunile de captură şi decodificare a informaţiilor din reţea, în Iris se pot defini diferite reguli de filtrare a monitorizării, se poate configura posibilitatea de înregistrare permanentă a traficului. IRIS poate fi configurat ca firewall, prin utilizarea setului propriu de reguli sau introducerea de noi reguli de monitorizare a accesului şi semnalarea sonoră a administratorului sistemului respectiv.

Partea cea mai interesantă la IRIS sînt sistemele de raportare grafică a activităţii defalcate pe diferite categorii sau intervale de timp. Aceste statistici pot fi personalizate din punctul de vedere al vizualizării : tip grafic, valori care să fie afişate, intervale de valori, afişare online etc.

După părerea noastră, IRIS este, în schimb, o aplicaţie care necesită resurse de memorie şi calcul destul de ridicate, mai ales în faza de decodificare a informaţiilor.

14.3. Utilitare pentru accesul la WMI

Una dintre cele mai interesante aplicaţii pentru accesul la resursele sistemului de operare este WMI Tools oferit de firma Microsoft, care este împărţit în 4 categorii :

- Object Browser ;
- CIM Studio ;
- Event Viewer ;
- Event Registration.

Folosind WMI, un utilizator experimentat poate vizualiza, modifica, elimina şi adăuga clase, obiecte, metode şi asociaţii în sistemul de operare.

Cunoscînd denumirea şi tipul diferitelor obiecte din sistemul de operare se pot crea diferite aplicaţii de configurare a acestuia, cea mai simplă metodă fiind aceea de creare a script-urilor de tip WHS, folosind limbajul VBS.

Un utilitar pentru scrierea şi depanarea script-urilor WHS este Microsoft Script Debugger care poate fi instalat o dată cu sistemul de operare sau ulterior, ca o componentă separată. O diferenţă esenţială faţă de Notepad este că oferă informaţii despre linia la care se află o eroare, şi aceasta poate fi localizată mai uşor, dar şi posibilitatea de execuţie pas cu pas a instrucţiunilor şi vizualizarea rezultatelor într-o fereastră de simulare.

14.4. Utilitare pentru conectarea la distanţă

În Windows 2000, utilitarul este Terminal Service Client ce permite conectarea la servere Windows 2000 care au instalat şi configurat serviciul Terminal Services. Conectarea se poate realiza în mod *application* (utilizatorul poate rula anumite aplicaţii specificate de administrator, instalate direct pe server), caz în care fiecare staţie de lucru trebuie să deţină o licenţă de acces (CAL - *Client Access Licence*), sau *remote administration* (utilizatorul se poate conecta de la distanţă la resursele unui server putînd efectua majoritatea operaţiunilor de administrare a acestuia).

Pentru conectarea de pe un sistem care are instalat sistemul de operare Windows 2000 Professional sau Server, trebuie instalată componenta Terminal Services Client, utilizînd 2 dischete de instalare care se creează de pe server:

1. **Start → Programs → Administrative Tools → Terminal Services Client Creator.**
2. Alegeţi tipul sistemului de operare pe care va rula clientul d-voastră: Windows pe 16 biţi (care se adresează sistemului de operare Windows for Workgroups 3.11, care rula pe sisteme vechi de tip 386), sau pe 32 de biţi, care se adresează sistemelor de operare mai noi.
3. Paşii anteriori pot fi depăşiţi prin copierea directă a fişierelor necesare instalării clientului de Terminal Services direct de la adresa: %windir%\system32\clients\tsclient\.
4. Instalaţi clientul rulînd aplicaţia *setup* de pe discul 1.
5. Pentru conectarea pe un server lansaţi Terminal Services Client (fig. 14.4.1) şi puteţi alege din listă serverul pe care doriţi să vă conectaţi precum şi dimensiunea ferestrei (*Screen area*).

Nu toţi utilizatorii dintr-o reţea se pot conecta în mod administrativ pe un server, ci numai cei cărora le-a fost configurat acest drept.

Pentru vizualizarea conectărilor la server în acest mod, accesaţi *Terminal Services Manager* din Administrative Tools din care puteţi vedea utilizatorii conectaţi, sesiunile deschise precum şi procesele pe care le rulează pe server. Operaţiunile pe care puteţi să le efectuaţi cu ajutorul acestui instrument sînt: oprirea unui proces,

trimiterea unui mesaj unui utilizator, deconectarea utilizatorului de pe server şi eliberarea conexiunii.

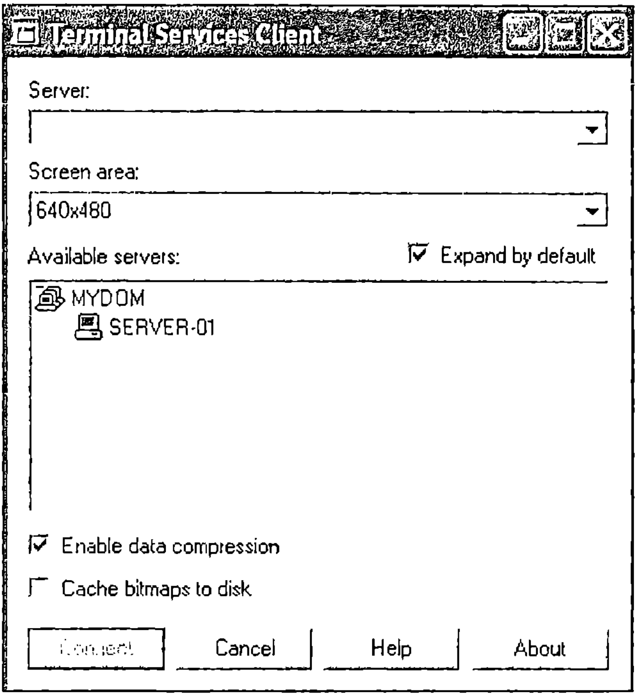


Figura 14.4.1. Fereastra de conectare la un anumit server

Un utilizator care se conectează de la distanţă poate lăsa deschisă o sesiune de lucru pe server, o a doua conectare aducînd utilizatorul în faţa aceluiaşi ecran ca în momentul deconectării de la server.

În Windows XP conectarea la distanţă se poate realiza cu ajutorul aplicaţiei Remote Desktop Sharing (fig. 14.4.2) pe care o găsiţi în Communications din Accessories.

Remote Desktop Connection este un utilitar mai avansat din prisma faptului că permite o conectare mai avansată la server, putînd avea acces la discurile locale, imprimante şi porturile seriale (opţiunea *Local Resources* din fig. 14.4.2.) direct din sesiunea deschisă pe server.

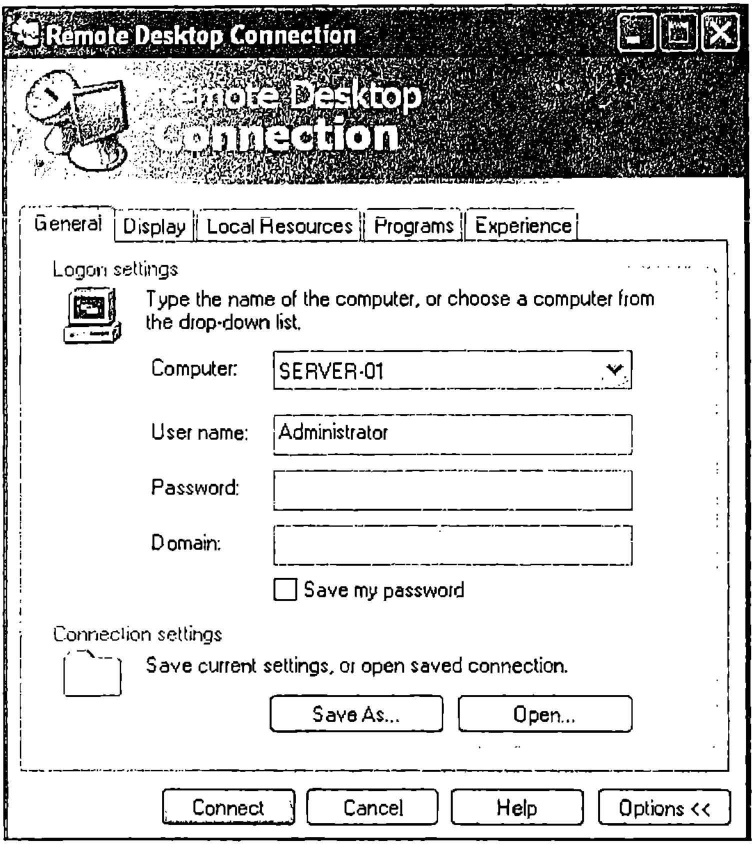


Figura 14.4.2. Fereastra de conectare de la distanță în Windows XP

14.5. Simulatoare şi instrumente de învăţare

VMware Workstation (VMware Inc.) este utilitar pentru simularea unei stații de lucru virtuale. Există versiuni pentru Windows şi Linux, putînd simula diferite sisteme de operare de la MS-DOS la Windows .NET Enterprise Server, Linux, NetWarem, FreBSD şi altele.

Configurarea unei stații virtuale (fig. 14.5.1) presupune alocarea unor resurse de pe stația reală: Memorie, spațiu pe hard disk, accesul la CD-ROM sau emularea unui CD-ROM virtual, accesul la unitatea de citire a dischetelor, acces la interfața de rețea, accesul la porturile USB şi, implicit, la dispozitivele conectate pe acesta.

Recomandată este utilizarea unei memorii RAM suplimentare în momentul în care se doreşte a se lucra cu VMware. Numărul maşinilor virtuale care pot fi create şi rulate în acelaşi timp pe un calculator real este limitat numai de resursele fizice ale acestuia din urmă.

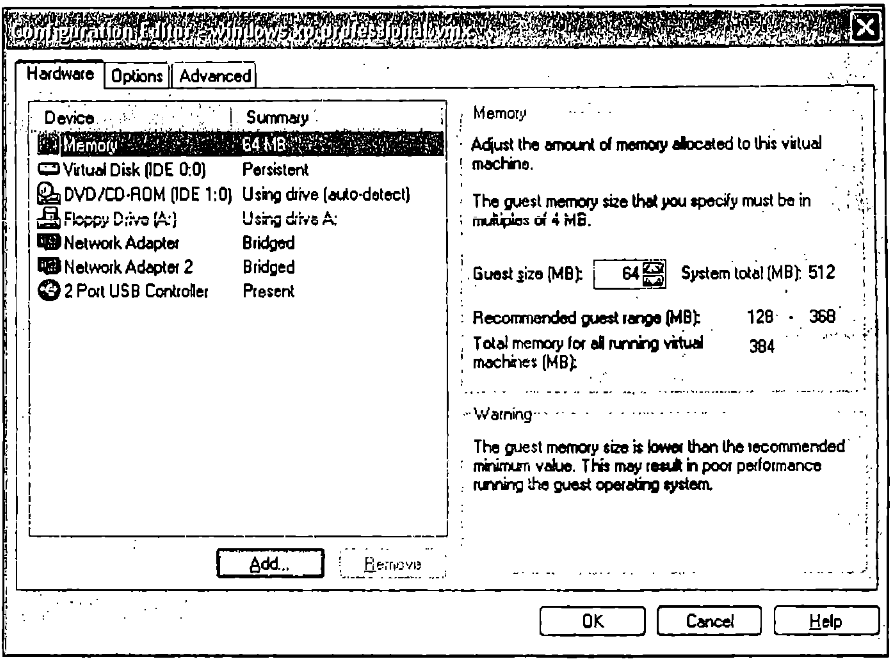


Figura 14.5.1. Configurarea dispozitivelor fizice aferente unui calculator virtual

Este unul dintre cele mai bune produse de acest gen şi îl recomandăm cu căldură pentru procesul de învăţare, experimentare, configurare şi utilizare a unor sisteme de operare noi. Dacă pe staţiile reale din aceeaşi reţea sînt instalate maşini virtuale care au configuraţii TCP/IP pentru aceeaşi reţea, calculatoarele virtuale comunică între ele prin intermediul interfeţelor de reţea a calculatoarelor reale, fără a exista o comunicare aparentă între real şi virtual. Calculatorul real nu răspunde la comanda ping lansată de pe calculatorul virtual.

O dată cu instalarea utilitarului se instalează automat încă două interfeţe de reţea logice: *VMware Virtual Ethernet Adapter (basic host-only support for VMnet1)*. şi *VMware Virtual Ethernet Adapter (Network Address Translation [NAT] for VMnet8)* care pot fi configurate împreună cu interfaţa de reţea fizică pentru a permite comunicarea între calculatorul virtual şi calculatorul fizic.

O altă facilitate este reprezentată de faptul că maşina virtuală este salvată într-un fişier cu extensia *.vmdk*, acesta putînd fi transferat pe alte staţii de lucru, sau multiplicarea unei staţii virtuale deja instalate şi configurate. Crearea copiilor de siguranţă vă asigură reluarea acţiunilor de configurare din momentul salvării, în cazul în care nu mai reuşiţi să reparaţi eventualele deteriorări logice ale sistemului.

RouterSim 3.0. Pentru partea de switching şi routing, aplicaţia lui Todd Lammle şi Bill Tedder este folosită în cadrul Academiilor CISCO şi pune la dispoziţia doritorilor un mediu de lucru foarte apropiat de realitate.

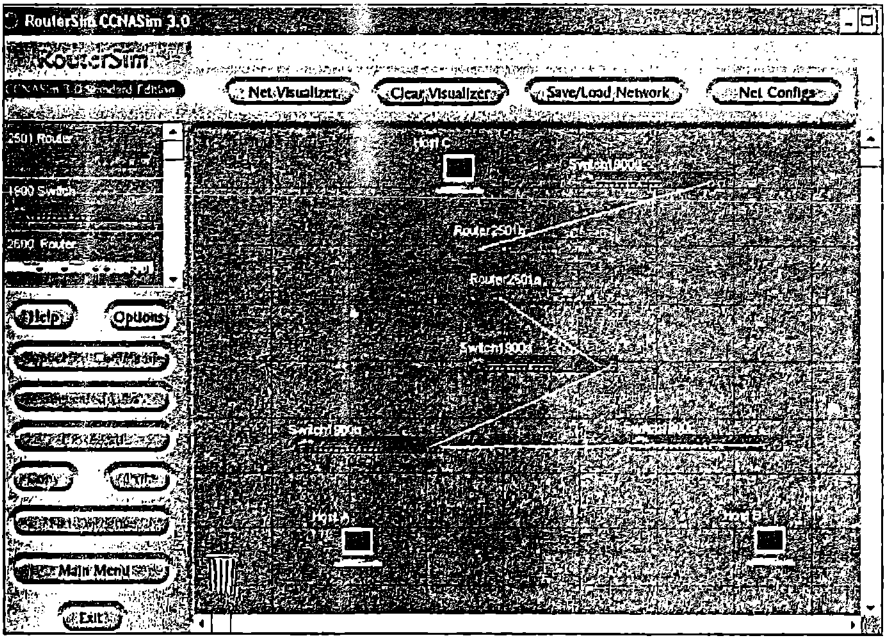


Figura 14.5.2. Router Sim 3.0

Pentru început se poate folosi topologia existentă și lecțiile oferite de aplicație. Dacă acest lucru nu vă mai mulțumește, puteți să vă creați propria topologie și să configurați echipamentele după cum credeți de cuviință. În caz de greșeli, aveți posibilitatea să obțineți un mic ajutor. Nu trebuie însă să uitați că lucrați cu un simulator care nu este capabil să emuleze toate comenzile unui IOS.

14.6. Instrumente de proiectare a rețelelor

Utilitarul oferit de Microsoft, *Visio*, nu este dedicat cu preponderență proiectării rețelelor de calculatoare, dar prin gama variată de opțiuni pe care le conține la categoria Network, putem spune cel puțin că se poate desena foarte bine o rețea.

Principalele tipuri de diagrame (fig. 14.6.1) care pot fi create în Visio pentru proiectarea unei rețele sînt:

- *Active directory* – pentru reprezentarea grafică a celor mai uzuale obiecte;
- *Basics Network* – pentru crearea unei diagrame a rețelei precum și pentru o documentare a acesteia;
- *LDAP Directory*;
- *Logical Network Diagram* – permite proiectarea detaliată a rețelelor;
- *Novell Directory Services*;
- *Visio Network Equipament Sampler* – conține un set de obiecte specifice Visio folosite în documentarea unei rețele.

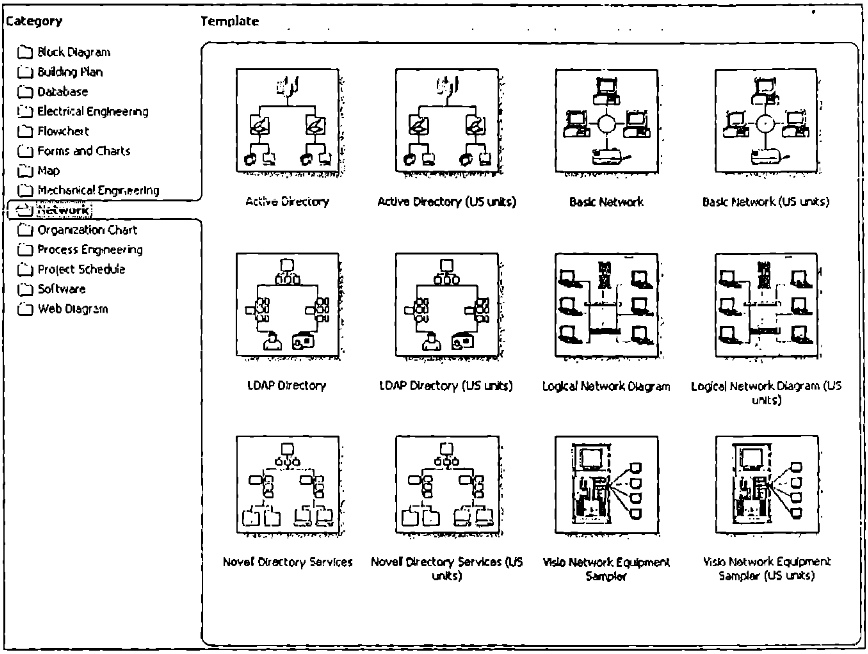


Figura 14.6.1. Alegerea unui anumit tip de diagramă

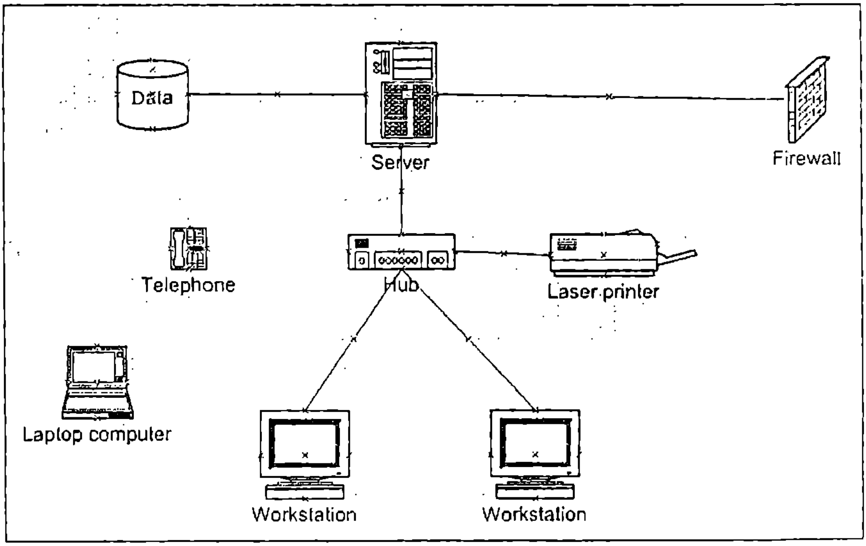


Figura 14.6.2. O diagramă de tip Basics Network

Pentru detalierea proprietăţilor fiecărui element dintr-o diagramă: RClick pe obiect → **Properties**. În fereastra *Custom Properties* pot fi completate o serie de informaţii standard, dar pot fi definite (butonul **Define**) alte proprietăţi pentru un anumit obiect, prin specificarea Numelui proprietăţii (*Name*), tipul informaţiei care va fi introdusă: string, number, date, boolean etc.

Visio oferă o serie de instrumente care pot fi accesate din meniul Tools:

- *Report* – utilitar pentru crearea şi vizualizarea unor rapoarte predefinite, care extrag anumite informaţii din obiectele din diagramă. Un raport predefinit poate fi modificat (butonul **Modify**) adăugîndu-i-se noi informaţii sau eliminînd altele. Afişarea unui raport (butonul **Run**) se poate realize în mai multe formate de documente: HTML, Excel, XML.
- *Export To Database* – utilitar pentru exportul informaţiilor dintr-o diagramă într-o bază de date, folosind conexiuni ODBC predefinite sau care pot fi create în această etapă.

Diagramele pot fi salvate ca documente Visio sau în alte formate: XML, AutoCAD, HTML, JPEG etc.

Netcracker Designer/Professional[1] *4.0*

Chiar dacă între timp această aplicaţie a devenit componentă a unei suite mai largi de soluţii pentru managementul infrastructurii IT dintr-o firmă, versiunea 4.0 a reprezentat un instrument excelent pentru proiectarea şi simularea traficului unei reţele de calculatoare.

Netcracker permite crearea de proiecte ierarhice pornind de la clădirea în care se realizează implementarea şi ajungînd la calculatorul sau rack-ul cu echipamente.

Principalele componente ale aplicaţiei sînt:

- *Project Hierarchy* – pentru vizualizarea ierarhiei componentelor proiectului;
- *Devices* – pentru selectarea echipamentelor ce se folosesc în cadrul proiectului;
- *Compatible devices* – vizualizarea echipamentelor compatibile.

Un proiect poate fi realizat numai folosind echipamente generice sau, atunci cînd se cunoaşte situaţia exactă, se pot selecta echipamentele de la producătorii doriţi. Dincolo de facilităţile de proiectare oferite, această aplicaţie poate realiza documentarea reţelei, bugetul acesteia, calculează şi alocă adrese IP acolo unde este cazul şi, nu în ultimul rînd, poate simula traficul în viitoarea reţea.

Reţeaua astfel proiectată se apropie cît mai mult de situaţia reală, fără a fi nevoit să ai la dispoziţie toate echipamentele.

1. Vezi www.netcracker.com.

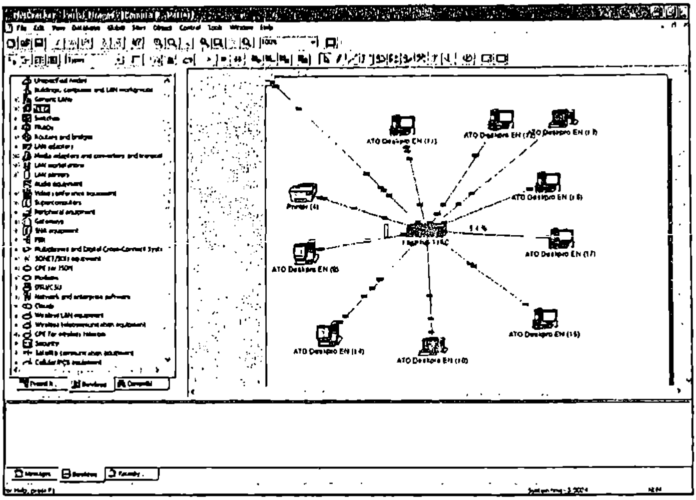


Figura 14.6.3. Utilitarul Netcraker Design

NetViz 6.0[1]

NetViz este o altă aplicaţie ce permite desenarea şi înregistrarea relaţiilor logice şi fizice dintre componentele unei reţele de calculatoare, sistem sau proces, precum şi descrierea acestor componente.

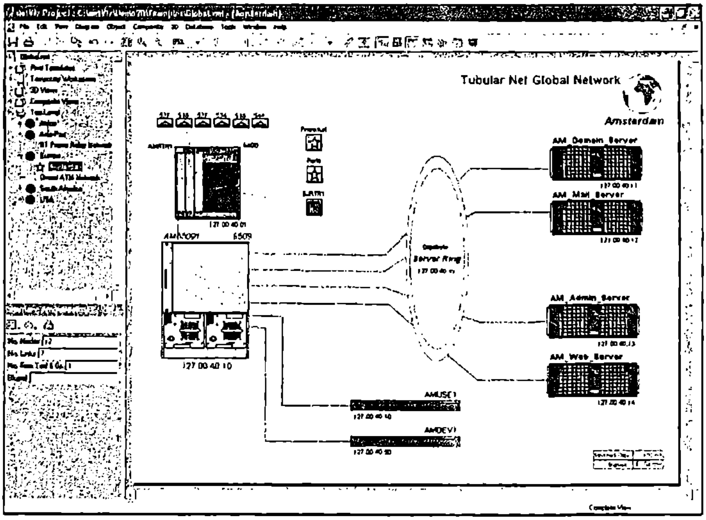


Figura 14.6.4. Utilitarul NetWiz 6.0

1. vezi www.netviz.com .

Ca şi în cazul Netcraker, elementul de bază al aplicaţiei îl reprezintă diagrama de reţea care poate fi un etaj, o clădire, un oraş etc.

Fiecare dintre aceste elemente poate fi considerat un nod cu subcomponente ce trebuie detaliate, cu posibilitatea de a vizualiza reţeaua în ansamblul său. Datele referitoare la echipamente pot fi vizualizate sau editate. Dacă datele despre reţea sînt memorate într-o bază de date sau într-un spreadsheet, pot fi importate pentru a popula diagrama de reţea din NetViz.

Nodurile şi legăturile folosite în cadrul unui proiect sînt definite în cadrul unui catalog ce poate exista separat de proiect.

Faţă de softul anterior, NetViz nu oferă posibilitatea simulării traficului în reţea, dar se poate face Telnet pe device-urile din diagrama construită.

CISCO ConfigMaker 2.6

Acesta este un utilitar proiectat pentru a configura prin intermediul unui PC reţele relativ mici în care se folosesc routere CISCO, switch-uri sau hub-uri.

Se porneşte de la realizarea diagramei de reţea şi configurarea fiecărui dispozitiv cu ajutorul wizard-urilor. Principalul avantaj constă în faptul că, spre deosebire de configurarea routerelor prin intermediul liniei de comenzi, în acest caz nu mai sînt necesare cunoştinţe despre IOS.

Aplicaţia realizează următoarele acţiuni:

- Detectează automat dispozitivele din reţea, folosind un port COM sau conexiunea de reţea de pe PC-ul pe care este instalată.
- Configurează protocoalele pentru rutare.
- Configurează rute statice.
- Configurează protocoalele rutabile.
- Realizează profile pentru firewall.
- Configurează VPN-uri.
- Distribuie configuraţiile realizate către respectivele dispozitive.

Din fericire, nu pot fi configurate decît anumite modele de echipamente. Pentru celelalte este nevoie de configurarea prin intermediul IOS-ului.

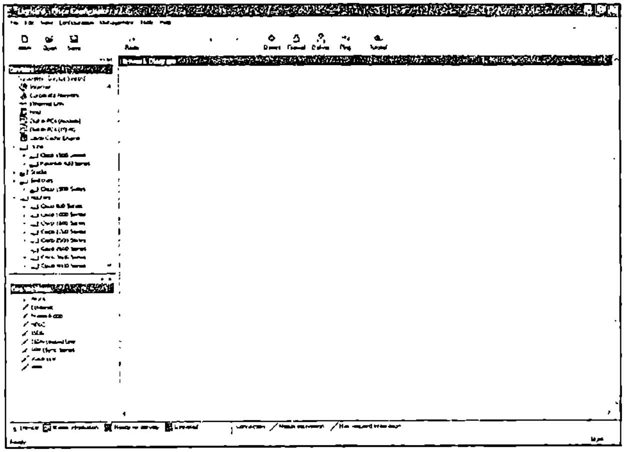


Figura 14.6.5. Utilitarul CISCO ConfigMaker 2.6

Anexă

255.255.255.0	255.255.254.0	255.255.252.0	255.255.248.0	255.255.240.0	255.255.224.0	255.255.128.0
172.16.0.0 - 172.16.0.255	172.16.0.0 - 172.16.1.255	172.16.0.0 - 172.16.3.255	172.16.0.0 - 172.16.7.255	172.16.0.0 - 172.16.15.255	172.16.0.0 - 172.16.31.255	160.69.0.0 - 160.69.127.255
172.16.1.0 - 172.16.1.255						
172.16.2.0 - 172.16.2.255	172.16.2.0 - 172.16.3.255					
172.16.3.0 - 172.16.3.255						
172.16.4.0 - 172.16.4.255	172.16.4.0 - 172.16.5.255	172.16.4.0 - 172.16.7.255				
172.16.5.0 - 172.16.5.255						
172.16.6.0 - 172.16.6.255	172.16.6.0 - 172.16.7.255					
172.16.7.0 - 172.16.7.255						
172.16.8.0 - 172.16.8.255	172.16.8.0 - 172.16.9.255	172.16.8.0 - 172.16.11.255	172.16.8.0 - 172.16.15.255			
172.16.9.0 - 172.16.9.255						
172.16.10.0 - 172.16.10.255	172.16.10.0 - 172.16.11.255					
172.16.11.0 - 172.16.11.255						
172.16.12.0 - 172.16.12.255	172.16.12.0 - 172.16.13.255	172.16.12.0 - 172.16.15.255				
172.16.13.0 - 172.16.13.255						
172.16.14.0 - 172.16.14.255	172.16.14.0 - 172.16.15.255					

255.255.255.0	255.255.254.0	255.255.252.0	255.255.248.0	255.255.240.0	255.255.224.0	255.255.128.0
172.16.15.0 - 172.16.15.255						
172.16.16.0 - 172.16.16.255	172.16.16.0 - 172.16.17.255	172.16.16.0 - 172.16.19.255	172.16.16.0 - 172.16.23.255	172.16.16.0 - 172.16.31.255		
172.16.17.0 - 172.16.17.255						
172.16.18.0 - 172.16.18.255	172.16.18.0 - 172.16.19.255					
172.16.19.0 - 172.16.19.255						
172.16.20.0 - 172.16.20.255	172.16.20.0 - 172.16.21.255	172.16.20.0 - 172.16.23.255				
172.16.21.0 - 172.16.21.255						
172.16.22.0 - 172.16.22.255	172.16.22.0 - 172.16.23.255					
172.16.23.0 - 172.16.23.255						
172.16.24.0 - 172.16.24.255	172.16.24.0 - 172.16.25.255	172.16.24.0 - 172.16.27.255	172.16.24.0 - 172.16.31.255			
172.16.25.0 - 172.16.25.255						
172.16.26.0 - 172.16.26.255	172.16.26.0 - 172.16.27.255					
172.16.27.0 - 172.16.27.255						
172.16.28.0 - 172.16.28.255	172.16.28.0 - 172.16.29.255	172.16.28.0 - 172.16.31.255				
172.16.29.0 - 172.16.29.255						
172.16.30.0 - 172.16.30.255	172.16.30.0 - 172.16.31.255					

255.255.255.0	255.255.254.0	255.255.252.0	255.255.248.0	255.255.240.0	255.255.224.0	255.255.128.0
172.16.31.0 - 172.16.31.255						
172.16.32.0 - 172.16.32.255	172.16.32.0 - 172.16.33.255	172.16.32.0 - 172.16.35.255	172.16.32.0 - 172.16.39.255	172.16.32.0 - 172.16.47.255	172.16.32.0 - 172.16.63.255	
172.16.33.0 - 172.16.33.255						
172.16.34.0 - 172.16.34.255	172.16.34.0 - 172.16.35.255					
172.16.35.0 - 172.16.35.255						
172.16.36.0 - 172.16.36.255	172.16.36.0 - 172.16.37.255	172.16.36.0 - 172.16.39.255				
172.16.37.0 - 172.16.37.255						
172.16.38.0 - 172.16.38.255	172.16.38.0 - 172.16.39.255					
172.16.39.0 - 172.16.39.255						
172.16.40.0 - 172.16.40.255	172.16.40.0 - 172.16.41.255	172.16.40.0 - 172.16.43.255	172.16.40.0 - 172.16.47.255			
172.16.41.0 - 172.16.41.255						
172.16.42.0 - 172.16.42.255	172.16.42.0 - 172.16.43.255					
172.16.43.0 - 172.16.43.255						
172.16.44.0 - 172.16.44.255	172.16.44.0 - 172.16.45.255	172.16.44.0 - 172.16.47.255				
172.16.45.0 - 172.16.45.255						
172.16.46.0 - 172.16.46.255	172.16.46.0 - 172.16.47.255					

255.255.255.0	255.255.254.0	255.255.252.0	255.255.248.0	255.255.240.0	255.255.224.0	255.255.128.0
172.16.47.0 - 172.16.47.255						
172.16.48.0 - 172.16.48.255	172.16.48.0 - 172.16.49.255	172.16.48.0 - 172.16.51.255	172.16.48.0 - 172.16.55.255	172.16.48.0 - 172.16.63.255		
172.16.49.0 - 172.16.49.255						
172.16.50.0 - 172.16.50.255	172.16.50.0 - 172.16.51.255					
172.16.51.0 - 172.16.51.255						
172.16.52.0 - 172.16.52.255	172.16.52.0 - 172.16.53.255	172.16.52.0 - 172.16.55.255				
172.16.53.0 - 172.16.53.255						
172.16.54.0 - 172.16.54.255	172.16.54.0 - 172.16.55.255					
172.16.55.0 - 172.16.55.255						
172.16.56.0 - 172.16.56.255	172.16.56.0 - 172.16.57.255	172.16.56.0 - 172.16.59.255	172.16.56.0 - 172.16.63.255			
172.16.57.0 - 172.16.57.255						
172.16.58.0 - 172.16.58.255	172.16.58.0 - 172.16.59.255					
172.16.59.0 - 172.16.59.255						
172.16.60.0 - 172.16.60.255	172.16.60.0 - 172.16.61.255	172.16.60.0 - 172.16.63.255				
172.16.61.0 - 172.16.61.255						
172.16.62.0 - 172.16.62.255	172.16.62.0 - 172.16.63.255					

255.255.255.0	255.255.254.0	255.255.252.0	255.255.248.0	255.255.240.0	255.255.224.0	255.255.128.0
172.16.63.0 - 172.16.63.255						
172.16.64.0 - 172.16.64.255	172.16.64.0 - 172.16.65.255	172.16.64.0 - 172.16.67.255	172.16.64.0 - 172.16.71.255	172.16.64.0 - 172.16.79.255	172.16.64.0 - 172.16.95.255	
172.16.65.0 - 172.16.65.255						
172.16.66.0 - 172.16.66.255	172.16.66.0 - 172.16.67.255					
172.16.67.0 - 172.16.67.255						
172.16.68.0 - 172.16.68.255	172.16.68.0 - 172.16.69.255	172.16.68.0 - 172.16.71.255				
172.16.69.0 - 172.16.69.255						
172.16.70.0 - 172.16.70.255	172.16.70.0 - 172.16.71.255					
172.16.71.0 - 172.16.71.255						
172.16.72.0 - 172.16.72.255	172.16.72.0 - 172.16.73.255	172.16.72.0 - 172.16.75.255	172.16.72.0 - 172.16.79.255			
172.16.73.0 - 172.16.73.255						
172.16.74.0 - 172.16.74.255	172.16.74.0 - 172.16.75.255					
172.16.75.0 - 172.16.75.255						
172.16.76.0 - 172.16.76.255	172.16.76.0 - 172.16.77.255	172.16.76.0 - 172.16.79.255				
172.16.77.0 - 172.16.77.255						
172.16.78.0 - 172.16.78.255	172.16.78.0 - 172.16.79.255					

255.255.255.0	255.255.254.0	255.255.252.0	255.255.248.0	255.255.240.0	255.255.224.0	255.255.128.0
172.16.79.0 - 172.16.79.255						
172.16.80.0 - 172.16.80.255	172.16.80.0 - 172.16.81.255	172.16.80.0 - 172.16.83.255	172.16.80.0 - 172.16.87.255	172.16.80.0 - 172.16.95.255		
172.16.81.0 - 172.16.81.255						
172.16.82.0 - 172.16.82.255	172.16.82.0 - 172.16.83.255					
172.16.83.0 - 172.16.83.255						
172.16.84.0 - 172.16.84.255	172.16.84.0 - 172.16.85.255	172.16.84.0 - 172.16.87.255				
172.16.85.0 - 172.16.85.255						
172.16.86.0 - 172.16.86.255	172.16.86.0 - 172.16.87.255					
172.16.87.0 - 172.16.87.255						
172.16.88.0 - 172.16.88.255	172.16.88.0 - 172.16.89.255	172.16.88.0 - 172.16.91.255	172.16.88.0 - 172.16.95.255			
172.16.89.0 - 172.16.89.255						
172.16.90.0 - 172.16.90.255	172.16.90.0 - 172.16.91.255					
172.16.91.0 - 172.16.91.255						
172.16.92.0 - 172.16.92.255	172.16.92.0 - 172.16.93.255	172.16.92.0 - 172.16.95.255				
172.16.93.0 - 172.16.93.255						
172.16.94.0 - 172.16.94.255	172.16.94.0 - 172.16.95.255					

255.255.255.0	255.255.254.0	255.255.252.0	255.255.248.0	255.255.240.0	255.255.224.0	255.255.128.0
172.16.95.0 - 172.16.95.255						
172.16.96.0 - 172.16.96.255	172.16.96.0 - 172.16.97.255	172.16.96.0 - 172.16.99.255	172.16.96.0 - 172.16.103.255	172.16.96.0 - 172.16.111.255	172.16.96.0 - 172.16.127.255	
172.16.97.0 - 172.16.97.255						
172.16.98.0 - 172.16.98.255	172.16.98.0 - 172.16.99.255					
172.16.99.0 - 172.16.99.255						
172.16.100.0 - 172.16.100.255	172.16.100.0 - 172.16.101.255	172.16.100.0 - 172.16.103.255				
172.16.101.0 - 172.16.101.255						
172.16.102.0 - 172.16.102.255	172.16.102.0 - 172.16.103.255					
172.16.103.0 - 172.16.103.255						
172.16.104.0 - 172.16.104.255	172.16.104.0 - 172.16.105.255	172.16.104.0 - 172.16.107.255	172.16.104.0 - 172.16.111.255			
172.16.105.0 - 172.16.105.255						
172.16.106.0 - 172.16.106.255	172.16.106.0 - 172.16.107.255					
172.16.107.0 - 172.16.107.255						
172.16.108.0 - 172.16.108.255	172.16.108.0 - 172.16.109.255	172.16.108.0 - 172.16.111.255				
172.16.109.0 - 172.16.109.255						
172.16.110.0 - 172.16.110.255	172.16.110.0 - 172.16.111.255					

255.255.255.0	255.255.254.0	255.255.252.0	255.255.248.0	255.255.240.0	255.255.224.0	255.255.128.0
172.16.111.0 - 172.16.111.255						
172.16.112.0 - 172.16.112.255	172.16.112.0 - 172.16.113.255	172.16.112.0 - 172.16.115.255	172.16.112.0 - 172.16.119.255	172.16.112.0 - 172.16.127.255		
172.16.113.0 - 172.16.113.255						
172.16.114.0 - 172.16.114.255	172.16.114.0 - 172.16.115.255					
172.16.115.0 - 172.16.115.255						
172.16.116.0 - 172.16.116.255	172.16.116.0 - 172.16.117.255	172.16.116.0 - 172.16.119.255				
172.16.117.0 - 172.16.117.255						
172.16.118.0 - 172.16.118.255	172.16.118.0 - 172.16.119.255					
172.16.119.0 - 172.16.119.255						
172.16.120.0 - 172.16.120.255	172.16.120.0 - 172.16.121.255	172.16.120.0 - 172.16.123.255	172.16.120.0 - 172.16.127.255			
172.16.121.0 - 172.16.121.255						
172.16.122.0 - 172.16.122.255	172.16.122.0 - 172.16.123.255					
172.16.123.0 - 172.16.123.255						
172.16.124.0 - 172.16.124.255	172.16.124.0 - 172.16.125.255	172.16.124.0 - 172.16.127.255				
172.16.125.0 - 172.16.125.255						
172.16.126.0 - 172.16.126.255	172.16.126.0 - 172.16.127.255					

255.255.255.0	255.255.254.0	255.255.252.0	255.255.248.0	255.255.240.0	255.255.224.0	255.255.128.0
172.16.127.0 172.16.127.255						
172.16.128.0 172.16.128.255	172.16.128.0 172.16.129.255	172.16.128.0 172.16.131.255	172.16.128.0 172.16.135.255	172.16.128.0 172.16.143.255	172.16.128.0 172.16.159.255	160.69.128.0 160.69.255.255
172.16.129.0 172.16.129.255						
172.16.130.0 172.16.130.255	172.16.130.0 172.16.131.255					
172.16.131.0 172.16.131.255						
172.16.132.0 172.16.132.255	172.16.132.0 172.16.133.255	172.16.132.0 172.16.135.255				
172.16.133.0 172.16.133.255						
172.16.134.0 172.16.134.255	172.16.134.0 172.16.135.255					
172.16.135.0 172.16.135.255						
172.16.136.0 172.16.136.255	172.16.136.0 172.16.137.255	172.16.136.0 172.16.139.255	172.16.136.0 172.16.143.255			
172.16.137.0 172.16.137.255						
172.16.138.0 172.16.138.255	172.16.138.0 172.16.139.255					
172.16.139.0 172.16.139.255						
172.16.140.0 172.16.140.255	172.16.140.0 172.16.141.255	172.16.140.0 172.16.143.255				
172.16.141.0 172.16.141.255						
172.16.142.0 172.16.142.255	172.16.142.0 172.16.143.255					

255.255.255.0	255.255.254.0	255.255.252.0	255.255.248.0	255.255.240.0	255.255.224.0	255.255.128.0
172.16.143.0 172.16.143.255						
172.16.144.0 172.16.144.255	172.16.144.0 172.16.145.255	172.16.144.0 172.16.147.255	172.16.144.0 172.16.151.255	172.16.144.0 172.16.159.255		
172.16.145.0 172.16.145.255						
172.16.146.0 172.16.146.255	172.16.146.0 172.16.147.255					
172.16.147.0 172.16.147.255						
172.16.148.0 172.16.148.255	172.16.148.0 172.16.149.255	172.16.148.0 172.16.151.255				
172.16.149.0 172.16.149.255						
172.16.150.0 172.16.150.255	172.16.150.0 172.16.151.255					
172.16.151.0 172.16.151.255						
172.16.152.0 172.16.152.255	172.16.152.0 172.16.153.255	172.16.152.0 172.16.155.255	172.16.152.0 172.16.159.255			
172.16.153.0 172.16.153.255						
172.16.154.0 172.16.154.255	172.16.154.0 172.16.155.255					
172.16.155.0 172.16.155.255						
172.16.156.0 172.16.156.255	172.16.156.0 172.16.157.255	172.16.156.0 172.16.159.255				
172.16.157.0 172.16.157.255						
172.16.158.0 172.16.158.255	172.16.158.0 172.16.159.255					

255.255.255.0	255.255.254.0	255.255.252.0	255.255.248.0	255.255.240.0	255.255.224.0	255.255.128.0
172.16.159.0 - 172.16.159.255						
172.16.160.0 - 172.16.160.255	172.16.160.0 - 172.16.161.255	172.16.160.0 - 172.16.163.255	172.16.160.0 - 172.16.167.255	172.16.160.0 - 172.16.175.255	172.16.160.0 - 172.16.191.255	
172.16.161.0 - 172.16.161.255						
172.16.162.0 - 172.16.162.255	172.16.162.0 - 172.16.163.255					
172.16.163.0 - 172.16.163.255						
172.16.164.0 - 172.16.164.255	172.16.164.0 - 172.16.165.255	172.16.164.0 - 172.16.167.255				
172.16.165.0 - 172.16.165.255						
172.16.166.0 - 172.16.166.255	172.16.166.0 - 172.16.167.255					
172.16.167.0 - 172.16.167.255						
172.16.168.0 - 172.16.168.255	172.16.168.0 - 172.16.169.255	172.16.168.0 - 172.16.171.255	172.16.168.0 - 172.16.175.255			
172.16.169.0 - 172.16.169.255						
172.16.170.0 - 172.16.170.255	172.16.170.0 - 172.16.171.255					
172.16.171.0 - 172.16.171.255						
172.16.172.0 - 172.16.172.255	172.16.172.0 - 172.16.173.255	172.16.172.0 - 172.16.175.255				
172.16.173.0 - 172.16.173.255						
172.16.174.0 - 172.16.174.255	172.16.174.0 - 172.16.175.255					

255.255.255.0	255.255.254.0	255.255.252.0	255.255.248.0	255.255.240.0	255.255.224.0	255.255.128.0
172.16.175.0 172.16.175.255						
172.16.176.0 172.16.176.255	172.16.176.0 172.16.177.255	172.16.176.0 172.16.179.255	172.16.176.0 172.16.183.255	172.16.176.0 172.16.191.255		
172.16.177.0 172.16.177.255						
172.16.178.0 172.16.178.255	172.16.178.0 172.16.179.255					
172.16.179.0 172.16.179.255						
172.16.180.0 172.16.180.255	172.16.180.0 172.16.181.255	172.16.180.0 172.16.183.255				
172.16.181.0 172.16.181.255						
172.16.182.0 172.16.182.255	172.16.182.0 172.16.183.255					
172.16.183.0 172.16.183.255						
172.16.184.0 172.16.184.255	172.16.184.0 172.16.185.255	172.16.184.0 172.16.187.255	172.16.184.0 172.16.191.255			
172.16.185.0 172.16.185.255						
172.16.186.0 172.16.186.255	172.16.186.0 172.16.187.255					
172.16.187.0 172.16.187.255						
172.16.188.0 172.16.188.255	172.16.188.0 172.16.189.255	172.16.188.0 172.16.191.255				
172.16.189.0 172.16.189.255						
172.16.190.0 172.16.190.255	172.16.190.0 172.16.191.255					

255.255.255.0	255.255.254.0	255.255.252.0	255.255.248.0	255.255.240.0	255.255.224.0	255.255.128.0
172.16.191.0 - 172.16.191.255						
172.16.192.0 - 172.16.192.255	172.16.192.0 - 172.16.193.255	172.16.192.0 - 172.16.195.255	172.16.192.0 - 172.16.199.255	172.16.192.0 - 172.16.207.255	172.16.192.0 - 172.16.223.255	
172.16.193.0 - 172.16.193.255						
172.16.194.0 - 172.16.194.255	172.16.194.0 - 172.16.195.255					
172.16.195.0 - 172.16.195.255						
172.16.196.0 - 172.16.196.255	172.16.196.0 - 172.16.197.255	172.16.196.0 - 172.16.199.255				
172.16.197.0 - 172.16.197.255						
172.16.198.0 - 172.16.198.255	172.16.198.0 - 172.16.199.255					
172.16.199.0 - 172.16.199.255						
172.16.200.0 - 172.16.200.255	172.16.200.0 - 172.16.201.255	172.16.200.0 - 172.16.203.255	172.16.200.0 - 172.16.207.255			
172.16.201.0 - 172.16.201.255						
172.16.202.0 - 172.16.202.255	172.16.202.0 - 172.16.203.255					
172.16.203.0 - 172.16.203.255						
172.16.204.0 - 172.16.204.255	172.16.204.0 - 172.16.205.255	172.16.204.0 - 172.16.207.255				
172.16.205.0 - 172.16.205.255						
172.16.206.0 - 172.16.206.255	172.16.206.0 - 172.16.207.255					

255.255.255.0	255.255.254.0	255.255.252.0	255.255.248.0	255.255.240.0	255.255.224.0	255.255.128.0
172.16.207.0 172.16.207.255						
172.16.208.0 172.16.208.255	172.16.208.0 172.16.209.255	172.16.208.0 172.16.211.255	172.16.208.0 172.16.215.255	172.16.208.0 172.16.223.255		
172.16.209.0 172.16.209.255						
172.16.210.0 172.16.210.255	172.16.210.0 172.16.211.255					
172.16.211.0 172.16.211.255						
172.16.212.0 172.16.212.255	172.16.212.0 172.16.213.255	172.16.212.0 172.16.215.255				
172.16.213.0 172.16.213.255						
172.16.214.0 172.16.214.255	172.16.214.0 172.16.215.255					
172.16.215.0 172.16.215.255						
172.16.216.0 172.16.216.255	172.16.216.0 172.16.217.255	172.16.216.0 172.16.219.255	172.16.216.0 172.16.223.255			
172.16.217.0 172.16.217.255						
172.16.218.0 172.16.218.255	172.16.218.0 172.16.219.255					
172.16.219.0 172.16.219.255						
172.16.220.0 172.16.220.255	172.16.220.0 172.16.221.255	172.16.220.0 172.16.223.255				
172.16.221.0 172.16.221.255						
172.16.222.0 172.16.222.255	172.16.222.0 172.16.223.255					

255.255.255.0	255.255.254.0	255.255.252.0	255.255.248.0	255.255.240.0	255.255.224.0	255.255.128.0
172.16.223.0 - 172.16.223.255						
172.16.224.0 - 172.16.224.255	172.16.224.0 - 172.16.225.255	172.16.224.0 - 172.16.227.255	172.16.224.0 - 172.16.231.255	172.16.224.0 - 172.16.239.255	172.16.224.0 - 172.16.255.255	
172.16.225.0 - 172.16.225.255						
172.16.226.0 - 172.16.226.255	172.16.226.0 - 172.16.227.255					
172.16.227.0 - 172.16.227.255						
172.16.228.0 - 172.16.228.255	172.16.228.0 - 172.16.229.255	172.16.228.0 - 172.16.231.255				
172.16.229.0 - 172.16.229.255						
172.16.230.0 - 172.16.230.255	172.16.230.0 - 172.16.231.255					
172.16.231.0 - 172.16.231.255						
172.16.232.0 - 172.16.232.255	172.16.232.0 - 172.16.233.255	172.16.232.0 - 172.16.235.255	172.16.232.0 - 172.16.239.255			
172.16.233.0 - 172.16.233.255						
172.16.234.0 - 172.16.234.255	172.16.234.0 - 172.16.235.255					
172.16.235.0 - 172.16.235.255						
172.16.236.0 - 172.16.236.255	172.16.236.0 - 172.16.237.255	172.16.236.0 - 172.16.239.255				
172.16.237.0 - 172.16.237.255						
172.16.238.0 - 172.16.238.255	172.16.238.0 - 172.16.239.255					

255.255.255.0	255.255.254.0	255.255.252.0	255.255.248.0	255.255.240.0	255.255.224.0	255.255.128.0
172.16.239.0 - 172.16.239.255						
172.16.240.0 - 172.16.240.255	172.16.240.0 - 172.16.241.255	172.16.240.0 - 172.16.243.255	172.16.240.0 - 172.16.247.255	172.16.240.0 - 172.16.255.255		
172.16.241.0 - 172.16.241.255						
172.16.242.0 - 172.16.242.255	172.16.242.0 - 172.16.243.255					
172.16.243.0 - 172.16.243.255						
172.16.244.0 - 172.16.244.255	172.16.244.0 - 172.16.245.255	172.16.244.0 - 172.16.247.255				
172.16.245.0 - 172.16.245.255						
172.16.246.0 - 172.16.246.255	172.16.246.0 - 172.16.247.255					
172.16.247.0 - 172.16.247.255						
172.16.248.0 - 172.16.248.255	172.16.248.0 - 172.16.249.255	172.16.248.0 - 172.16.251.255	172.16.248.0 - 172.16.255.255			
172.16.249.0 - 172.16.249.255						
172.16.250.0 - 172.16.250.255	172.16.250.0 - 172.16.251.255					
172.16.251.0 - 172.16.251.255						
172.16.252.0 - 172.16.252.255	172.16.252.0 - 172.16.253.255	172.16.252.0 - 172.16.255.255				
172.16.253.0 - 172.16.253.255						
172.16.254.0 - 172.16.254.255	172.16.254.0 - 172.16.255.255					
172.16.255.0 - 172.16.255.255						

Bibliografie

1. Bagnall B., Russell R., *E-Mail Virus Protection Handbook,* Syngress, 2000.
2. Cepeda O., *Beyond DHCP-Work Your TCP/IP Internetwork with Dynamic IP*, Ed. IBM Redbooks, 2000.
3. Derfler F. ; Les Freed, *How Networks Work - Fourth Edition*, Macmillan Computer Publishing, 1998.
4. Dunsmore B., Brown W. J., *Internet Security*, Syngress, 2000.
5. Fisher D., Vilas S., Hermance M., *Power Networking Second Edition : 59 Secrets for Personal & Professional Success*, Bard Press ; 2000.
6. Geihs K., Konig W., Von Westarp F., *Networks*, Ed. Physica-Verlag Heidelberg, New York, 2002.
7. Held G., *Handbook of Communications Systems Management*, CRC Press LLC, 1999.
8. Irvine J., Harle D., *Data Communications and Networks*, Joh Wiley&Sons, 2002.
9. Kosiur D., *Building and Managing Virtual Private Networks*, John Wiley & Son, 1998.
10. Kurose F.J., Ross W.K., *Computer Networking. A Top-Down Approach Featuring the Internet*, Addison Wesley, 2003.
11. Mann T.C., Terplan K., *Network Design : Management and Technical Perspectives*, CRC Press LLC, 1998.
12. Noam E.M., *Interconnecting the Network of Networks*, Ed. MIT Press, Cambridge, 2001.
13. Odom W., *Cisco CCNA Exam →640-607 Certification Guide,* Cisco Press, 2002.
14. Ogletree T., *Upgrading and Repairing Network - 3rd Edition*, Que, 2001.
15. Oppenheimer P., *Top-Down Network Design,* Cisco Press, 1999.
16. Oprea D., *Managementul proiectelor. Teorie şi cazuri practice*, Ed. Sedcom Libris, Iaşi, 2001.
17. Oprea D., *Protecţia şi securitatea sistemelor informaţionale*, Ed. Polirom, Iaşi, 2002.
18. Perlman R., *Interconnections : Bridges, Routers, Switches and Internetworking Protocols*, Addison-Wesley Pub Co., 1999.
19. Peterson L., Davie B., *Reţele de calculatoare*, Ed. All Educational, Bucureşti, 2000.
20. Russell R., Cunningham S., *Hack Proofing your Network*, Syngress, 2000.
21. Seifert R., *The Switch Book : The Complete Guide to LAN Switching Technology*, John Wiley & Sons ; 2000.
22. Skoudis E., *Counter Hack : A Step-by-Step Guide to Computer Attacks and Effective Defenses*, Prentice Hall PTR ; 2001.
23. Slone J.P., *Handbook of Local Area Networks*, CRC Press LLC, 1998.
24. Spurgeon C.E., *Ethernet : The Definitive Guide*, O'Reilly, 2000.
25. Stallings W., *Local and Metropolitan Area Networks (6th Edition)*, Prentice Hall ; 2000.
26. Tanenbaum A.S., *Reţele de calculatoare*, Computer Pres Agora, 1996.

http : //techrepublic.com.

http : //searchWin2000.com.

Microsoft TechNet – Script Center – http : //www.microsoft.com/technet/itsolutions/howto/acthow.asp.

http : //www.devguru.com.

http : //www.webopalia.com.

http : //www.wbatis.com.

La Editura POLIROM

au apărut :

Emanuela Cerchez – *Internet. Utilizarea rețelei Internet. Proiectarea paginilor Web* (manual opțional pentru liceu)
Emanuela Cerchez, Marinel Șerban – *Informatica pentru gimnaziu*
Doina Hrinciuc Logofătu – *C++. Probleme rezolvate și algoritmi*
Emanuela Cerchez – *Informatica. Culegere de probleme pentru liceu*
Emanuela Cerchez – *Internet. Manual pentru liceu*
Silvia Curteanu – *PC. Ghid de utilizare*
Emanuela Cerchez, Marinel Șerban – *PC. Pas cu pas*
Marin Fotache – *SQL. Dialecte DB2, Oracle și Visual FoxPro*
Cristina Perhinschi, Petronela Ilucă – *Word. Simplu și eficient*
Sabin Buraga – *Proiectarea siturilor Web. Design și funcționalitate*
Călin Ioan Acu – *Optimizarea paginilor Web*
Liliana Arici – *Informatică. Caiet de lucru pentru clasa a V-a*
Ana Întuneric, Cristina Sichim – *Informatică. Teste grilă. C, C++*
Mircea Băduț – *Calculatorul în trei timpi*
Elena Nechita, Gabriela-Cerasela Crișan – *PC pentru toți*
Adrian Munteanu, Valerică Greavu Șerban – *Rețele locale de calculatoare*

www.polirom.ro

Redactor: Mihai-Silviu Chirilă
Coperta: Ionuț Broștianu
Tehnoredactor: Gabriela Ghețău

Bun de tipar: octombrie 2003. Apărut: 2003
Editura Polirom, B-dul Carol I nr. 4 • P.O. Box 266
700506, Iași, Tel. & Fax: (0232) 21.41.00 ; (0232) 21.41.11 ;
(0232) 21.74.40 (difuzare) ; E-mail: office@polirom.ro
București, B-dul I.C. Brătianu nr. 6, et. 7, ap. 33,
O.P. 37 • P.O. Box 1-728, 030174
Tel.: (021) 313.89.78 ; E-mail: polirom@dnt.ro

Tiparul executat la S.C. LUMINA TIPO s.r.l.
str. Luigi Galvani nr. 20 bis, sect. 2, București
Tel./Fax: 211.32.60, 212.29.27, E-mail: lumina-lex@fx.ro